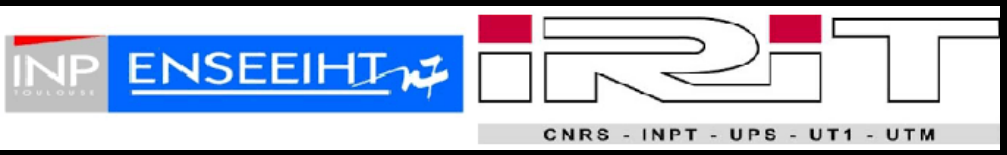


Sécurité dans le cloud computing

Alain Tchana, Maître de Conférence -
alain.tchana@enseeiht.fr
N7 (enseignement), IRIT (recherche) - Toulouse

Université de Toulouse

La sécurité est crucial dans ce monde tout numérique

La cyberattaque WannaCry a coûté 1 Md USD à l'économie mondiale

CC BY 2.0 / elhombredenegro / Crackers

INTERNATIONAL 08:58 25.05.2017 (mis à jour 11:09 25.05.2017) URL courte

Dossier: Cyberattaque Wannacry (11) 0 388 1 2

Les pertes causées par la cyberattaque sans précédent WannaCry s'élèvent à un milliard de dollars. L'attaque a touché plusieurs pays, établissements et sociétés de premier plan

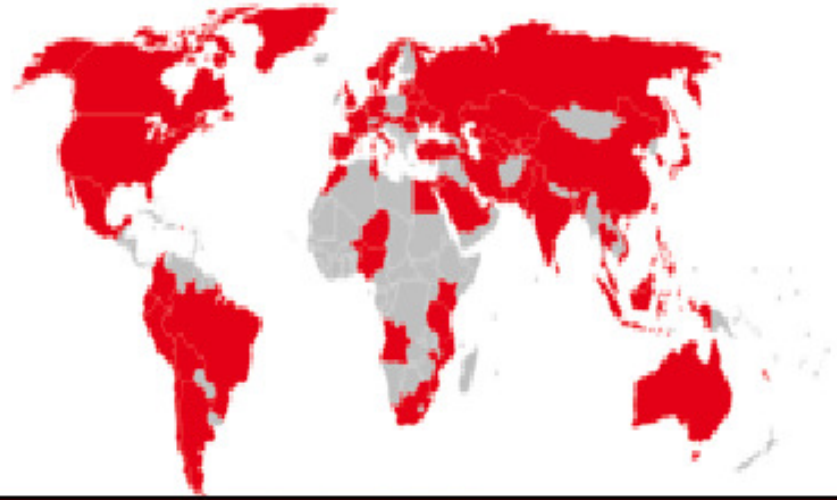
ACTUALITÉS

LES PLUS RÉCENTS | LES PLUS LUS | LES PLUS COMMENTÉS

17:15 **44 États US refusent de fournir à la Commission Trump les données sur les élections**

La sécurité est crucial dans ce monde tout numérique

Mai 2017



You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special

HIGH-TECH Cyberattaque mondiale en cours: NotPetya pourrait être pire que WannaCry

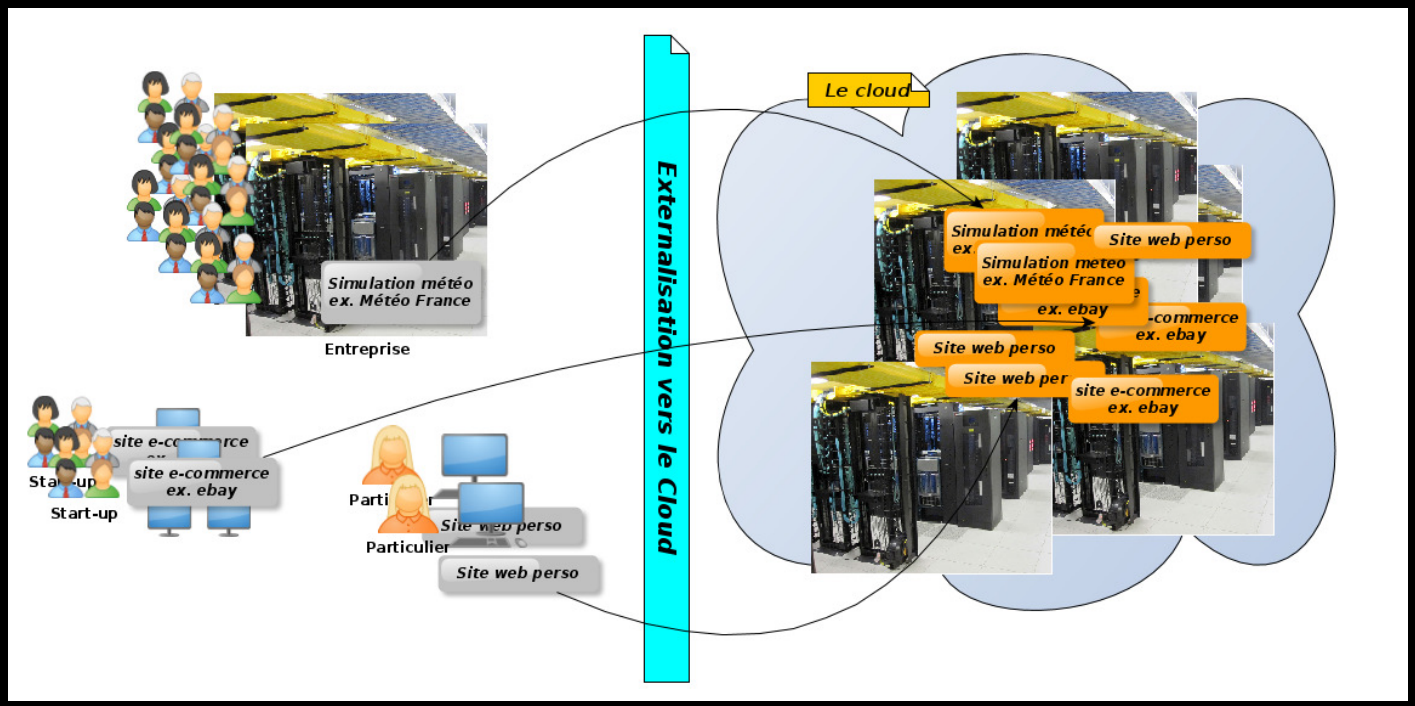
ACCUEIL › HIGH-TECH

Cyberattaque mondiale en cours: NotPetya pourrait être pire que WannaCry

Cloud computing

Principe de base

- Mutuatlisation et Multi-tenant
- Allocation à la demande et Paiement à l'usage

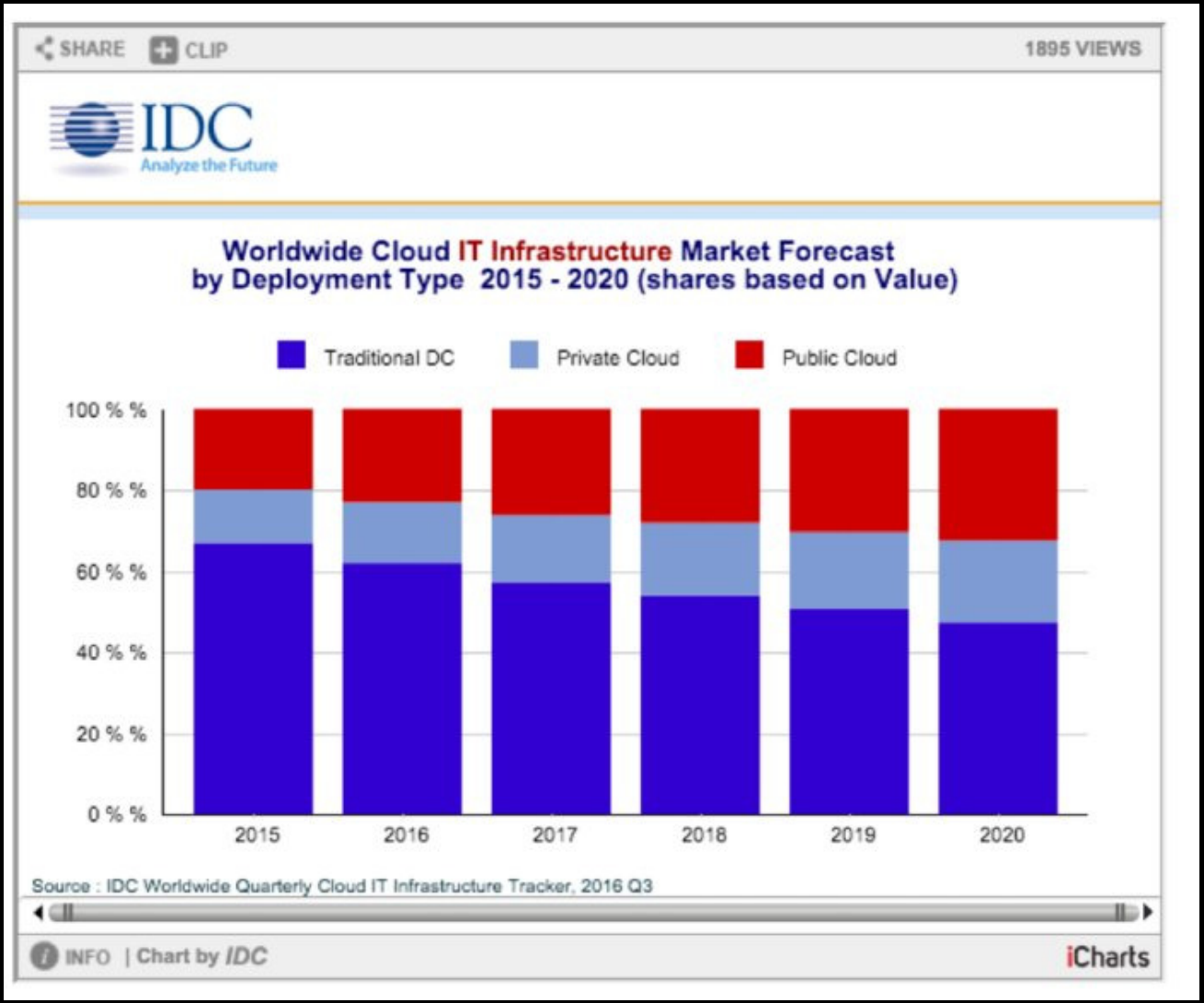


Quelques chiffres

D'une étude menée par l'IDC (International Data Corporation) en 2015

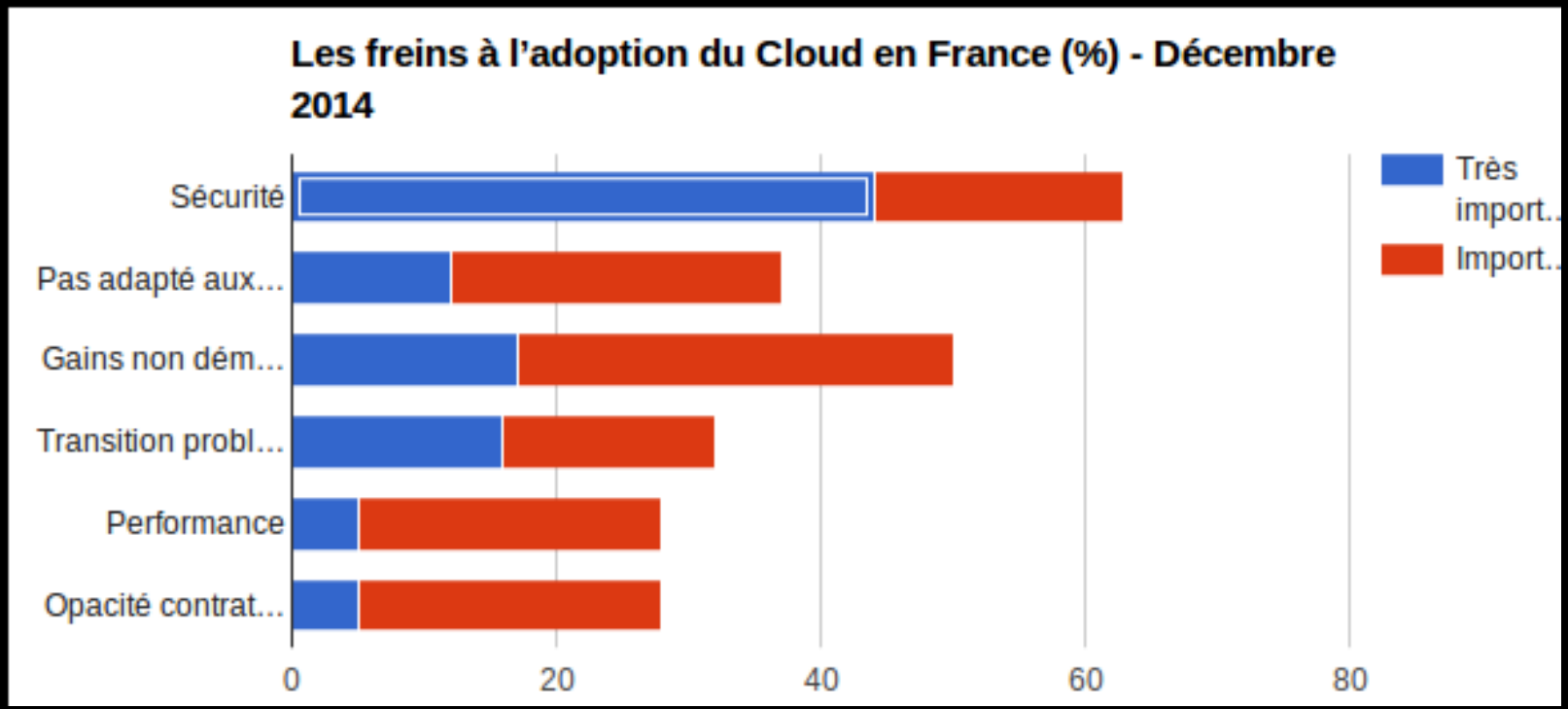
- 53% des entreprises pensent que le cloud va augmenter leurs revenus en l'espace de deux ans
- Une utilisation optimale apporte les gains suivants
  - Augmentation du chiffre d'affaires de 10%
  - Réduction des coûts de l'IT de 77%
  - Réduction du délai de provisionnement des services et applications de 99%
  - etc.

Quelques chiffres

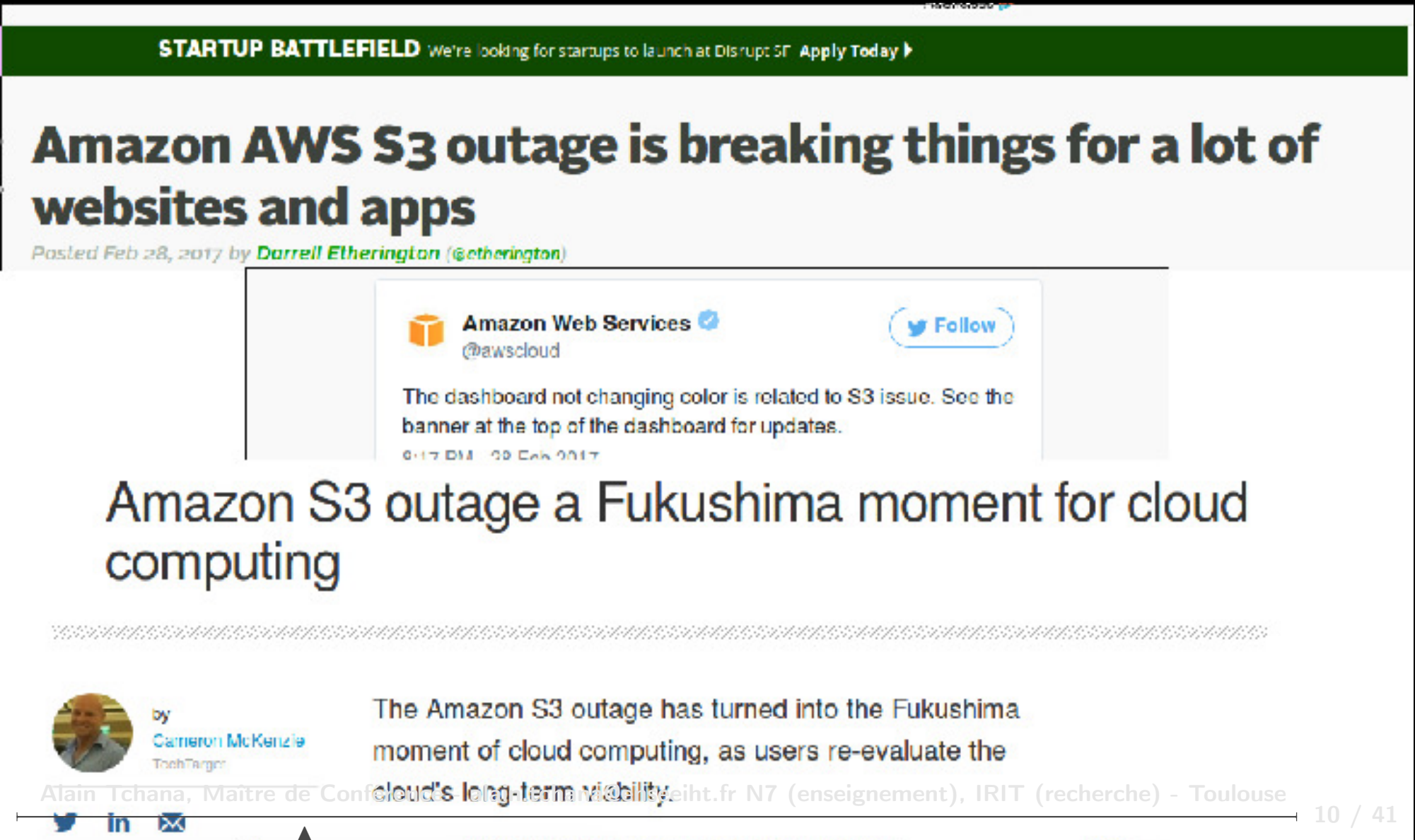


Défis dans le cloud

- Impact énergetique
- Garantie de service
- Standardisation
- –Sécurité–



De graves conséquences



STARTUP BATTLEFIELD We're looking for startups to launch at Disrupt SF Apply Today

Amazon AWS S3 outage is breaking things for a lot of websites and apps

Posted Feb 28, 2017 by Darrell Etherington (@etherington)

Amazon Web Services
@awscloud

Follow

The dashboard not changing color is related to S3 issue. See the banner at the top of the dashboard for updates.

Amazon S3 outage a Fukushima moment for cloud computing

by Cameron McKenzie
TechTarget

The Amazon S3 outage has turned into the Fukushima moment of cloud computing, as users re-evaluate the cloud's long-term viability.

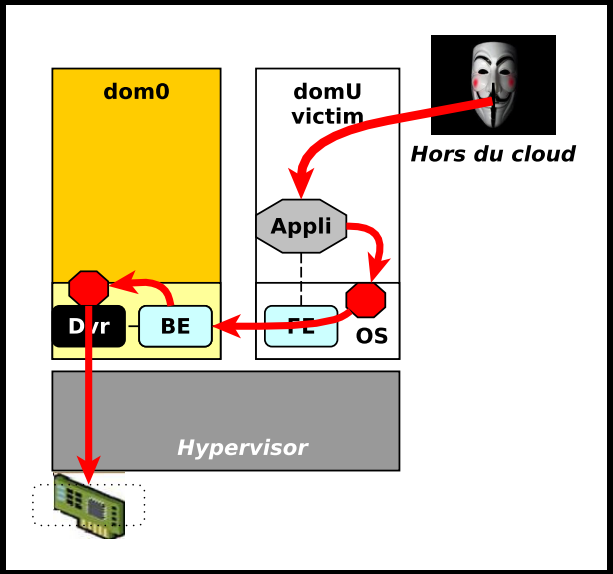
De graves conséquences

This is by no means an exhaustive list of things that fell over or were wobbly today, due to the S3 downtime, but here's a start: Docker's Registry Hub, Trello, Travis CI, GitHub and GitLab, Quora, Medium, Signal, Slack, Imgur, Twitch.tv, Razer, heaps of publications that stored images and other media in S3, Adobe's cloud, Zendesk, Heroku, Coursera, Bitbucket, Autodesk's cloud, Twilio, Mailchimp, Citrix, Expedia, Flipboard, and Yahoo! Mail (which you probably shouldn't be using anyway). Readers also reported that Zoom.us and some Salesforce.com services were having problems, as were Xero, SiriusXM, and Strava. Another reader reports being unable to order coffee because the Hey You app was broken.

La ménace

Externe

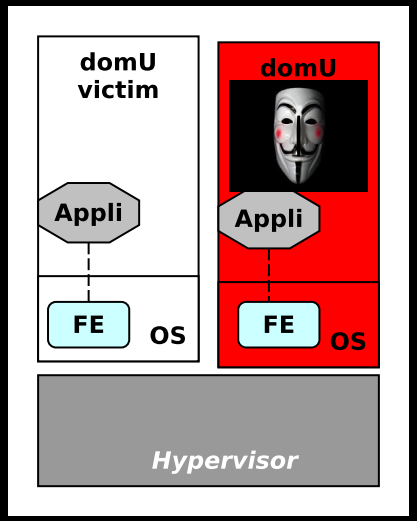
- Attaque classique d'applications
- Deni de service
- Sniffer le réseaux



La ménace

Un autre client

- Possibilité d'avoir le concurrent dans le même cloud
- Possibilité d'avoir un hacker dans le cloud
- $\Rightarrow$ espionnage du voisin



La ménace

Le Fournisseur et ses employés

- Le fournisseur peut revendre des informations
- La loi peut contraindre le fournisseur à divulguer les données
- Un employé mal intentionné ou pas

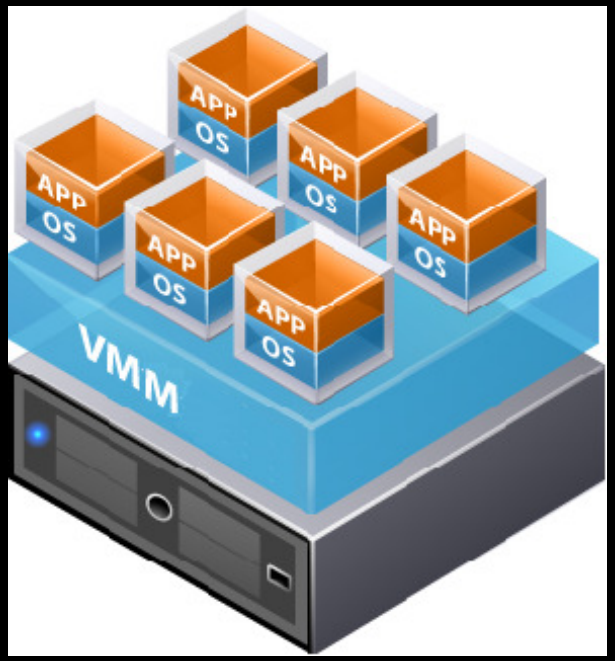
Attaques physiques

- Catastrophes naturelles: (coupure d'électricité dans un datacenter d'Amazon 12 Juin 2009)
- Quid des attaques terroriste

Les solutions de sécurité

Attaque par un client

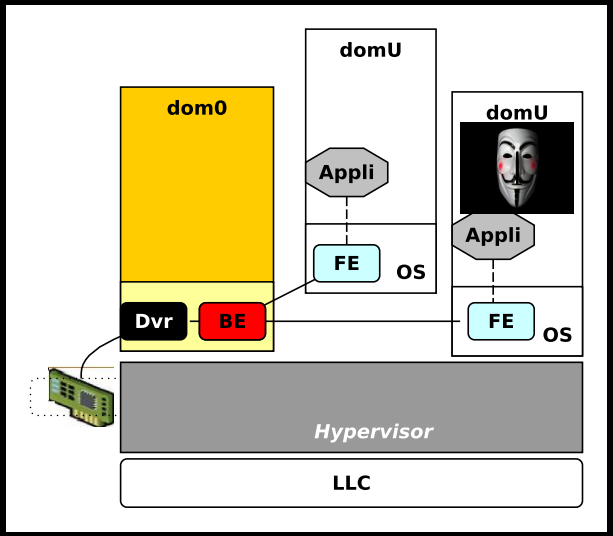
- Utilisation de la virtualisation/containerisation
  - l'isolation des ressources
  - l'isolation des espaces d'utilisation
  - l'isolation des défaillances



Les solutions de sécurité

Limites de la virtualisation

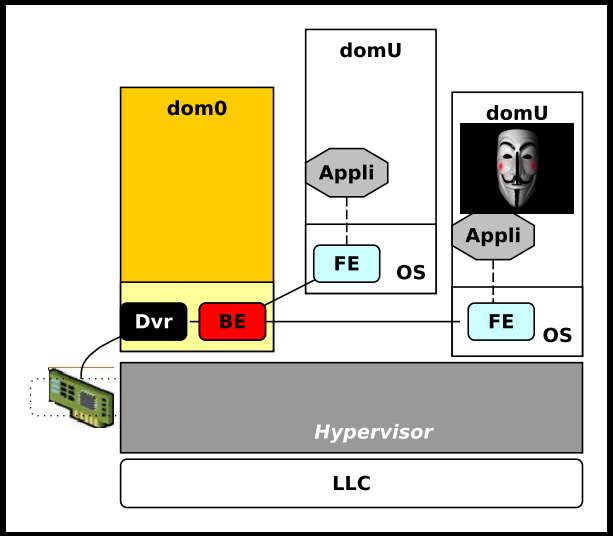
- Micro-ressources (cache) non isolées. Voir "Bolt: I Know What You Did Last Summer...In the Cloud" [ASPLOS 2017]
- Composants de l'hyperviseur non isolés. Voir "An Experimental Study of Cascading Performance Interference in a Virtualized Environment" SIGMETRICS 2013



Les solutions de sécurité

Limites de la virtualisation

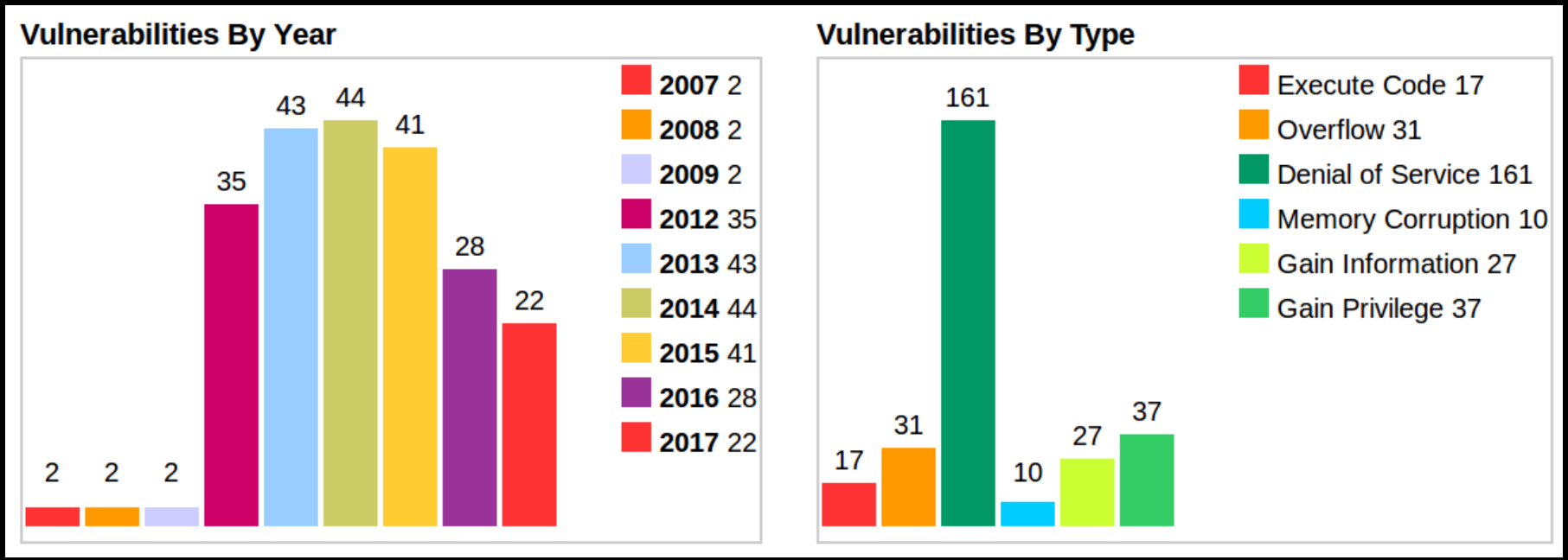
- Micro-ressources (cache) non isolées
  - Début de solution: Intel CAT (Cache Allocation Technology)
- Composants de l'hyperviseur non isolés
  - Début de solution: Intel VT-d



Les solutions de sécurité

Limites de la virtualisation

- Des vulnérabilités dans le code source
  - Xen hypervisor: 184 vulnerabilities (2012-2016)
  - Linux kernel: 721 vulnerabilities (2012-2016)



Les solutions de sécurité

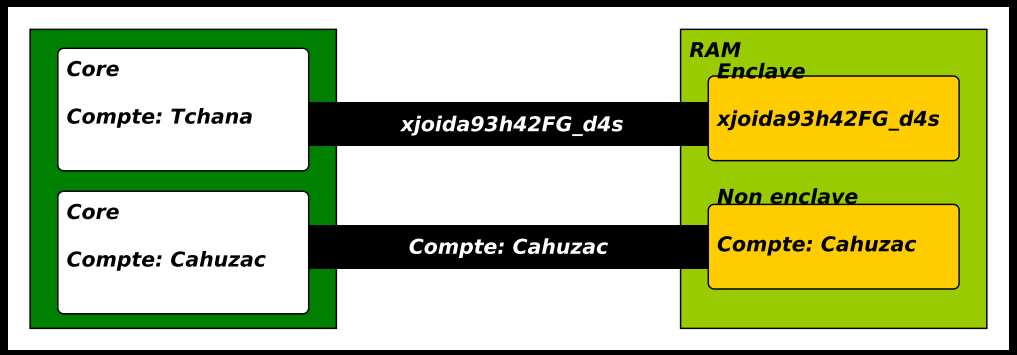
Attaque par le fournisseur ou ses employés

- Utilisation de la cryptographie (chiffrer les données)
  - Mais une fois en mémoire, les données seront déchiffrées, donc visible
  - Bus snooping
- Utilisation de SGX (Software guard extensions)
  - Présent dans les derniers processeurs Intel: Skylake (2015), Kaby lake (2016)
  - Protection à la fois des données et des applications
  - Le déchiffrement ne se fait que dans le processeur

Les solutions de sécurité

Focus sur SGX

- La portion de mémoire chiffrée s'appelle "***enclave***".
- Uniquement le code qui se trouve dans l'enclave peut accéder à l'enclave.
- Le déchiffrement dans le processeur (Intel).
- Même un accès physique à la machine (e.g. les bus de données) ne permet pas de voir les données.



Les solutions de sécurité

Programmer des enclaves

- Acquerir une machine avec des processeurs SGX-enabled
- Activer SGX via le BIOS
- Sous Windows
  - Installer MS Visual Studio Professional 2012
  - Installer Intel Platform Software and SDK
- Linux: download and build Platform Software and SDK (https://github.com/01org/linux-sgx)

Les solutions de sécurité

Quelques concepts et cycle de vie de l'enclave

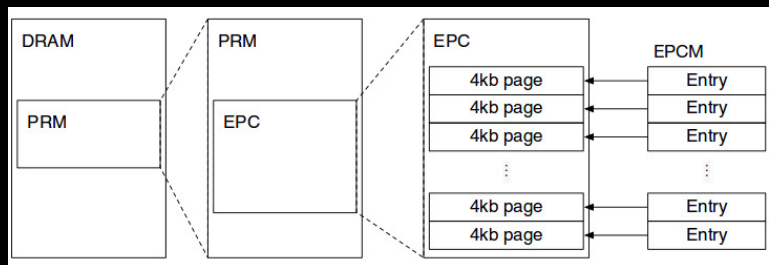
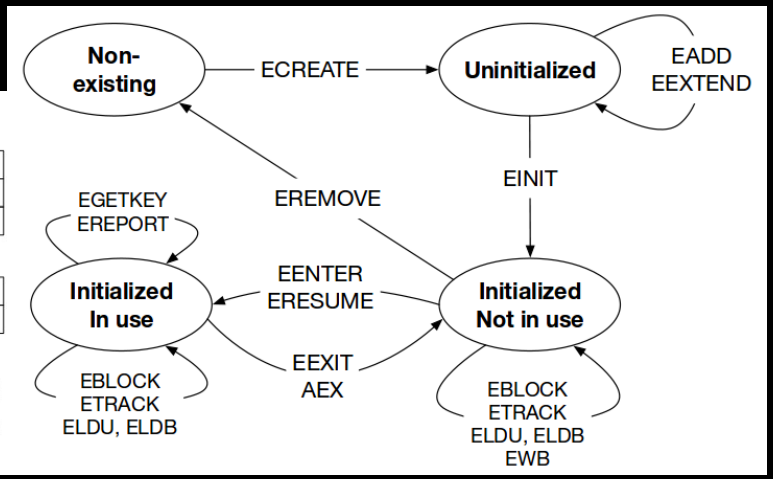


Figure 60: Enclave data is stored into the EPC, which is a subset of the PRM. The PRM is a contiguous range of DRAM that cannot be accessed by system software or peripherals.



- EENTER pour démarrer l'exécution du code dans l'enclave
- EEXIT pour terminer l'exécution
- Ces deux instructions doivent être exécutées en Ring 3

Les solutions de sécurité

SGX application: unstrusted code

```
char request_buf[BUFFER_SIZE];
char response_buf[BUFFER_SIZE];

int main()
{
 ...
 while(1)
 {
  receive(request_buf);
  ret = EENTER(request_buf, response_buf);
  if (ret < 0)
   fprintf(stderr, "Corrupted message\n");
  else
   send(response_buf);
 }
 ...
}
```

Enclave: trusted code

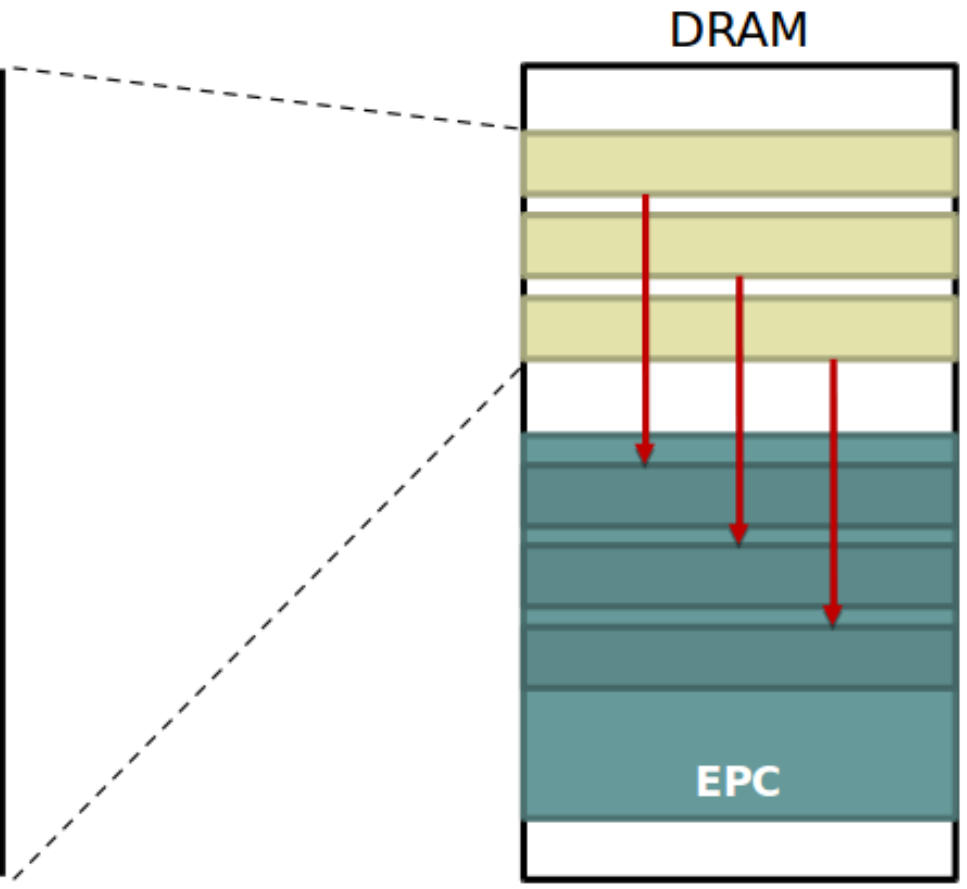
```
char input_buf[BUFFER_SIZE];
char output_buf[BUFFER_SIZE];

int process_request(char *in, char *out)
{
 copy_msg(in, input_buf);
 if(verify_MAC(input_buf))
 {
  decrypt_msg(input_buf);
  process_msg(input_buf, output_buf);
  encrypt_msg(output_buf);
  copy_msg(output_buf, out);
  EEXIT(0);
 } else
  EEXIT(-1);
}
```

Les solutions de sécurité

```
char input_buf[BUFFER_SIZE];
char output_buf[BUFFER_SIZE];

int process_request(char *in, char *out)
{
 copy_msg(in, input_buf);
 if(verify_MAC(input_buf))
 {
  decrypt_msg(input_buf);
  process_msg(input_buf, output_buf);
  encrypt_msg(output_buf);
  copy_msg(output_buf, out);
  EEXIT(0);
 } else
  EEXIT(-1);
}
```



Les solutions de sécurité

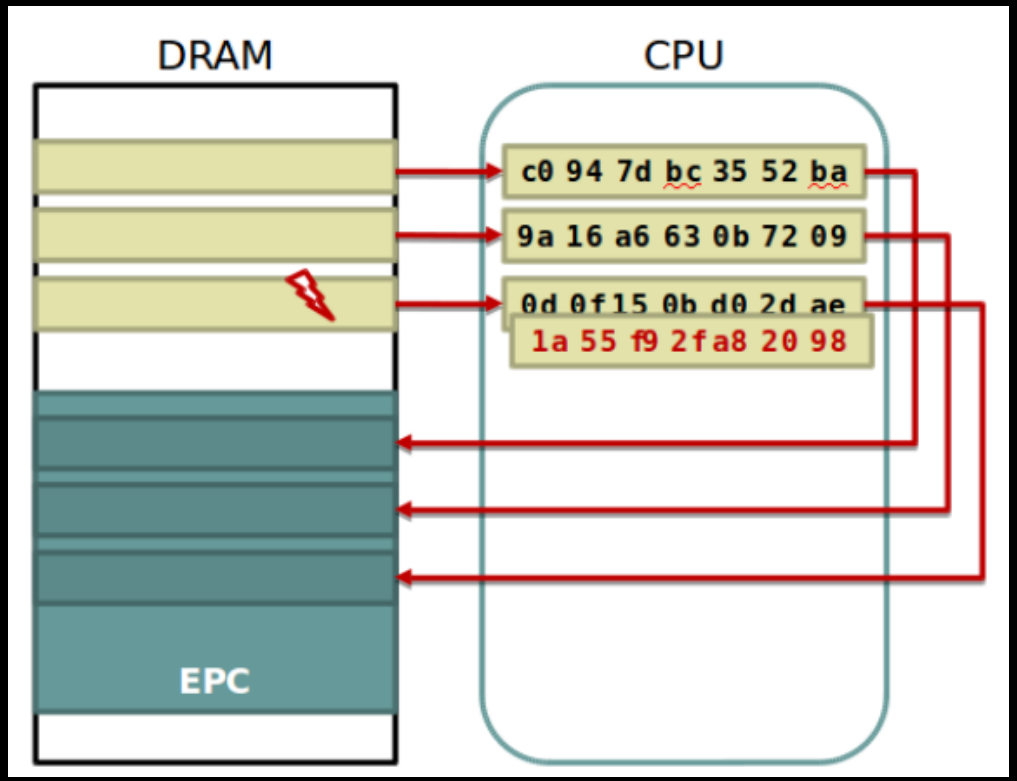
```
int process_request(char *in, char *out)
{
 copy_msg(in, input_buf);
 if(verify_MAC(input_buf))
 {
  decrypt_msg(input_buf);
  process_msg(input_buf, output_buf);
  encrypt_msg(output_buf);
  copy_msg(output_buf, out);
  EEXIT(0);
 } else
  EEXIT(-1);
}
```

```
int process_request(char *in, char *out)
{
 copy_msg(in, input_buf);
 if(verify_MAC(input_buf))
 {
  decrypt_msg(input_buf);
  process_msg(input_buf, output_buf);
  copy_msg(output_buf, external_buf);
  encrypt_msg(output_buf);
  copy_msg(output_buf, out);
  EEXIT(0);
 } else
  EEXIT(-1);
}
```

Les solutions de sécurité

Attestation de l'enclave

- Est ce que mon code qui s'exécute à distance est intact?
- Attestation locale ou distante



Les solutions de sécurité

Focus sur SGX: les limites

- Des bugs de sécurité déjà (6 bugs aux dernières nouvelles), voir https://www.intel.com/content/dam/www/public/us/en/documents/updates/desktop-6th-gen-core-family-spec-update.pdf

SKL012	The SMSW Instruction May Execute Within an Enclave
Problem	The SMSW instruction is illegal within an SGX (Software Guard Extensions) enclave, and an attempt to execute it within an enclave should result in a #UD (invalid-opcode exception). Due to this erratum, the instruction executes normally within an enclave and does not cause a #UD.
Implication	The SMSW instruction provides access to CR0 bits 15:0 and will provide that information inside an enclave. These bits include NE, ET, TS, EM, MP and PE.
Workaround	None identified. If SMSW execution inside an enclave is unacceptable, system software should not enable SGX.
Status	For the steppings affected, see the Summary Table of Changes.

Les solutions de sécurité

Focus sur SGX: les limites

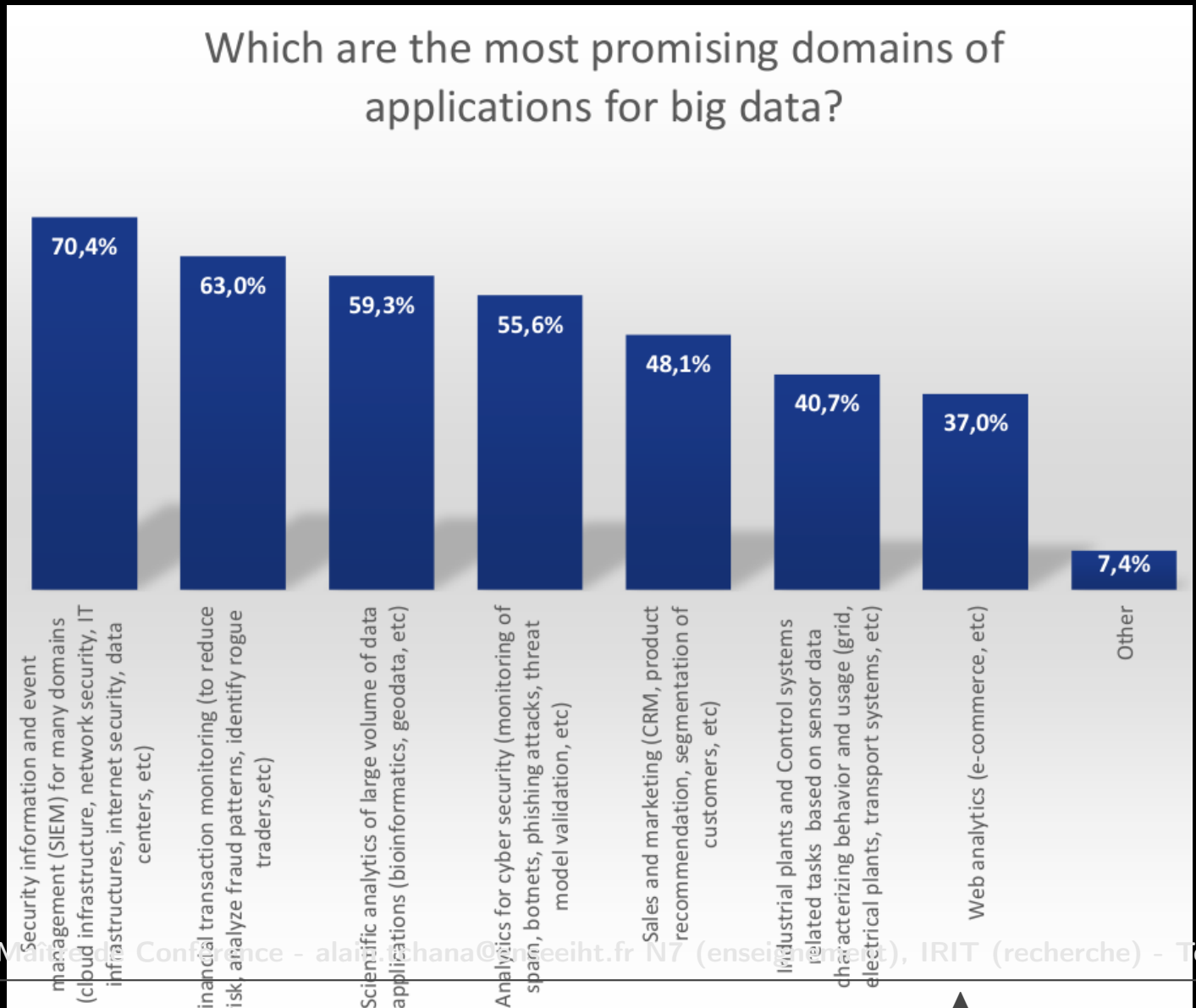
- La taille de l'enclave est limitée
  - uniquement 128MB
  - 96MB pour les utilisateurs, le reste pour les metadata
- Les entrées et sorties de l'enclave ont un impact sur les performances
- La gestion de l'enclave (pagination) est très coûteuse en performance
- Plus important: Intel détient le monopole
  - Ceci peut constituer une ménace (car entreprise étrangère)

Les solutions de sécurité

Attaque d'utilisateurs externes

- Utilisation de la virtualisation/containerisation
- Utilisation des firewall (e.g. Web Application Firewall ou encore "Security group" chez Amazon).
- Le big data
  - Permet au fournisseur d'anticiper des attaques (détection des patterns, PCA par exemple)

Les solutions de sécurité



Les solutions de sécurité

Attaque de terroristes et catastrophes

- Réplication des données à travers plusieurs data centers
- Constructions renforcées
  - Exemple du Cloud SAP: "The data center consists of 100,000 metric tons of reinforced concrete and rests on 480 concrete pillars, each extending 16 meters into the ground. The exterior walls are 30 centimeters thick and made of reinforced concrete. The server rooms are further surrounded by 3 concrete walls. This design provides effective protection against storms and even a small airplane crash."

Les solutions de sécurité

Respecter les normes et récommandations

- Norme ISO 27001 pour les data centers en général
- Norme ISO/IEC 27018 en complément pour les clouds
- Des récommandations basiques
  - Controller l'access physique au data center: "A lot of people will forget the physical because there is so much on the network side" Corbin Miller de la NASA.
  - Bien séparer les data centers de production des data centers R&D.
  - Régulièrement scanner les vulnerabilités des applications (utilisation de IBM Rational AppScan pour les apps. web par exemple)

Les solutions de sécurité

Respecter les normes et récommandations

- Suivre les trainings pour la certification CCSK
- Se tenir à jour des rapports d'organismes qui traitent de la sécurité
  - ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information)
  - Cloud Security Alliance

Qui est responsable de quoi?

IaaS

- Le client: application, données et système d'exploitation
- Le fournisseur: hyperviseur, machine physique, locaux

PaaS

- Le client: données, une partie des applications
- Le fournisseur: une partie des applications, système d'exploitation, hyperviseur, machine physique, locaux

SaaS

- Le client: rien
- Le fournisseur: tout

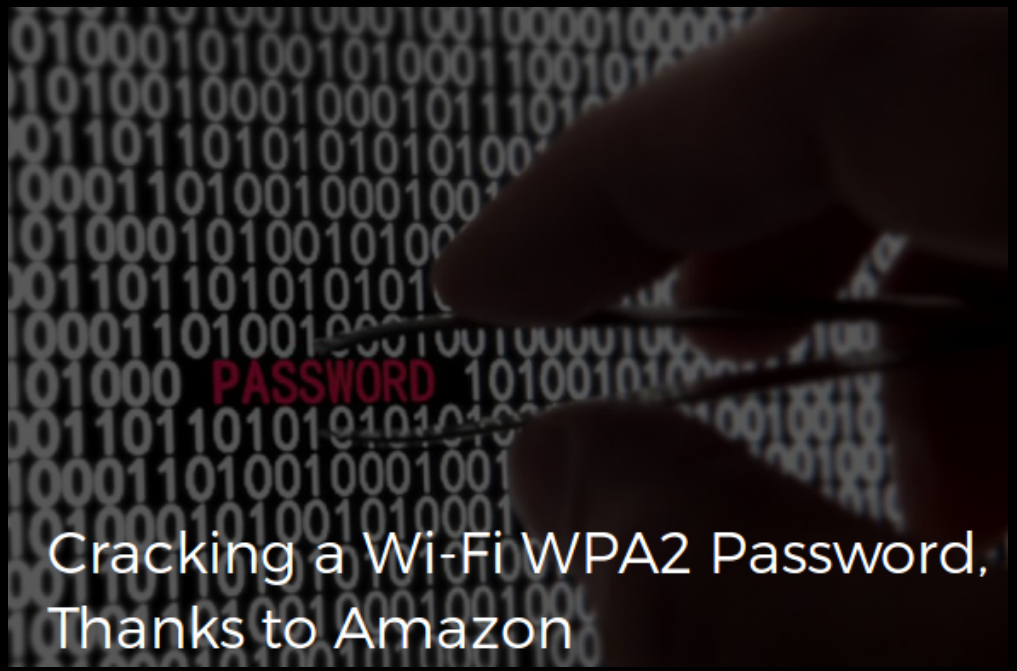
Conclusion

- Le cloud est très attractif
  - Concentration de plusieurs entreprises
- Cible privilégiée pour des attaques
- Plusieurs sources d'attaques
- Il existe des solutions encourageantes (SGX), malgré quelques limitations

Perspectives

Une forme de ménace reste ouverte

- Le cloud est souvent utilisé pour mener des actions malveillantes dont les victimes sont hors du cloud



Perspectives

Une forme de ménace reste ouverte

- Utilisation par des terrosites pour faire transiter des données discrètement

Fin

- Merci pour votre attention
- (Merci à Pascal Felber, Pr. Neuchatel - Suisse, pour la partie SGX)
- "*Un ordinateur en sécurité est un ordinateur éteint. Et encore...*" Bill Gates.