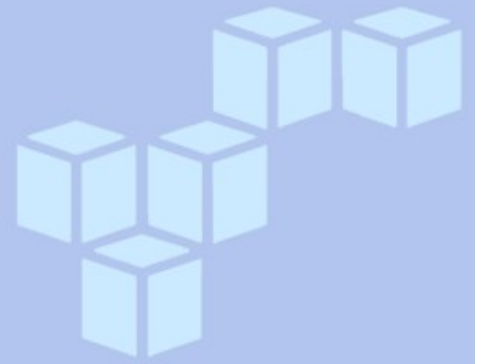
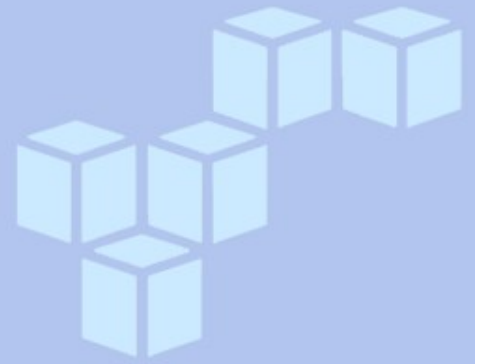
AWS Access Keys

w szerszym kontekście



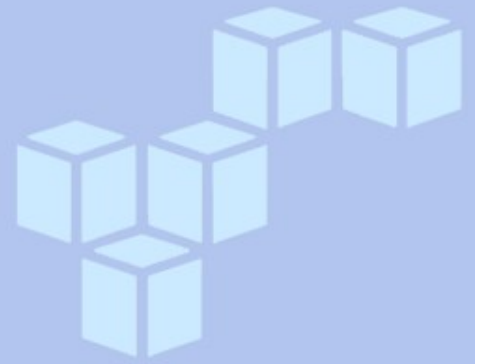
Grzegorz Grad

System Inżynier w Zespole
Utrzymania Infrastruktury
DataCenter z Allegro



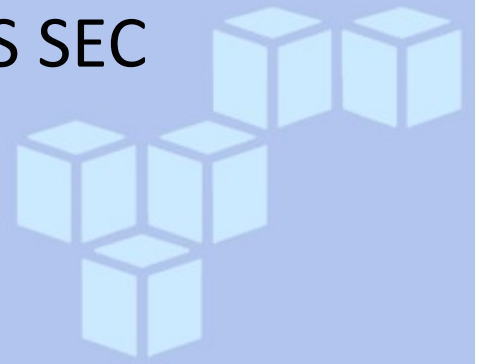
Agenda

- Wprowadzenie
- Przypadek użycia
- Dostęp do AWS – Root , IAM
- Jak powstaje chaos
- Czy to nie tylko paranoja „Bezpieczników”
- Uprawnienia kolejne starcie
- Czy coś zyskaliśmy ?
- Pytania



Wprowadzenie

- Wirtualny przypadek użycia.
- Chaos
  - Część z własnego doświadczenia
  - Sporo z rozmów korytarzowych
  - Trochę wiedzy z AWS Summit
- Finał
  - Trochę wiedzy z AWS Summit
  - Trochę wiedzy ze szkoleń AWS SA i AWS SEC
  - I sporo godzin z przypadkami z życia

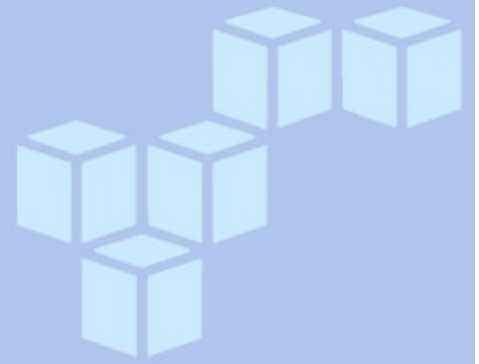


Przypadek użycia

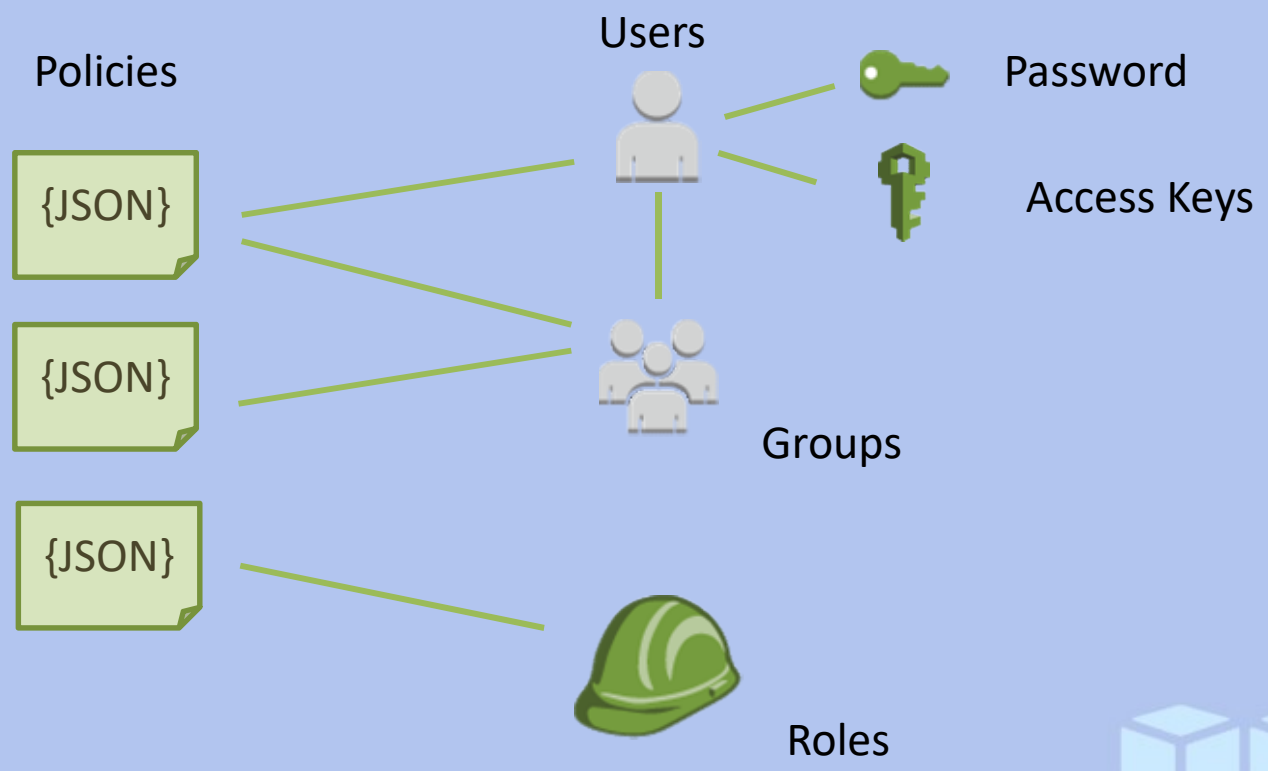
- Mikro-usługi (w on-premises)
  - Każda korzysta z różnych serwisów AWS (po API)
  - Każdą utrzymuje 2 dev i 2 adm
- Firma zatrudnia średnio 20 dev i 10 adm
- Firma ma 10 kont AWS
- Firma ma 100 usług
- Pracownicy migrują są zwalniani i zatrudniani nowi

IAM

- Czy wiemy do czego służą :
  - IAM (Identity and Access Management)
  - MFA (multi-factor authentication)
  - Konto Root
  - Access Keys

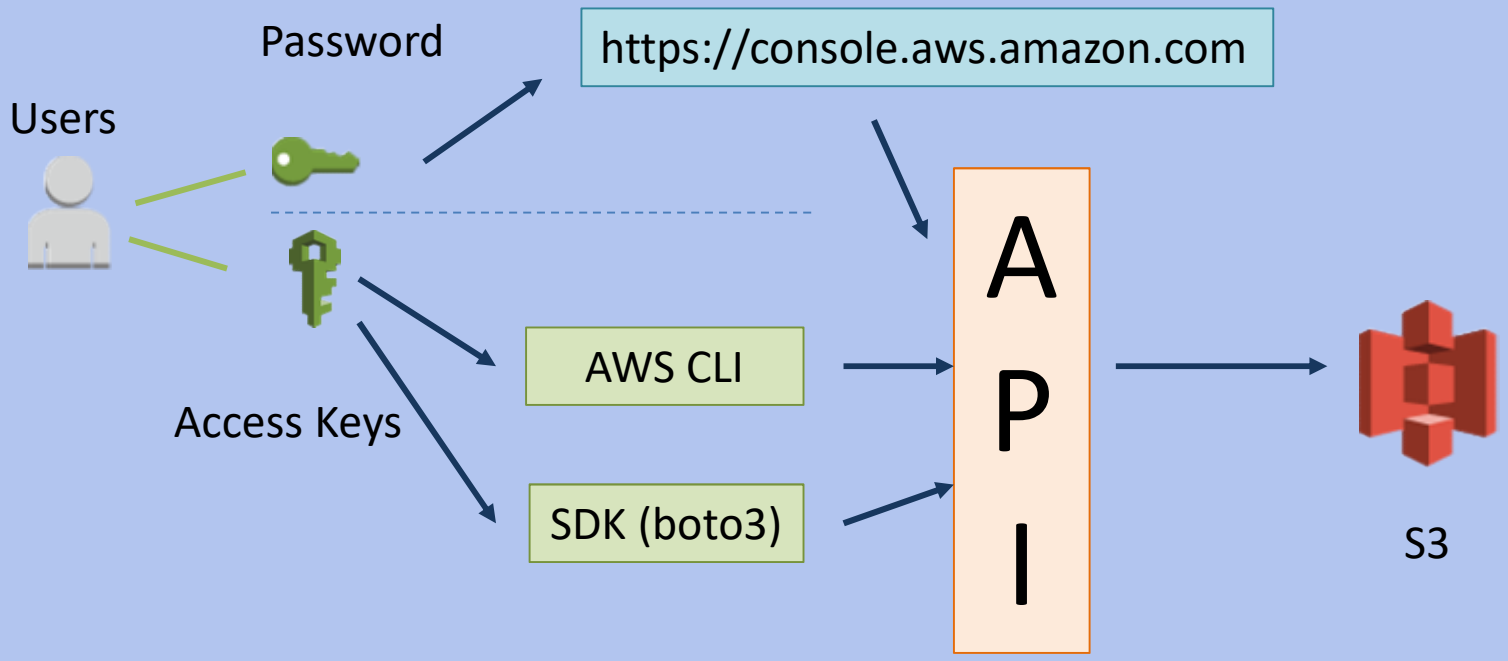


IAM + Access Keys



MzIzNzJjMzJjM2UyOGY5YzNiZTdlNjBlYjdlZDQyOWNkZTUzNTI5N2UzYTljYzc0ZTg1NTRkOWI3MzIzNzJjMzJjM2UyOGY5YzN

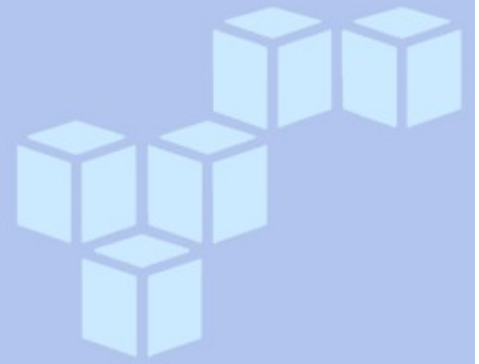
IAM + Access Keys



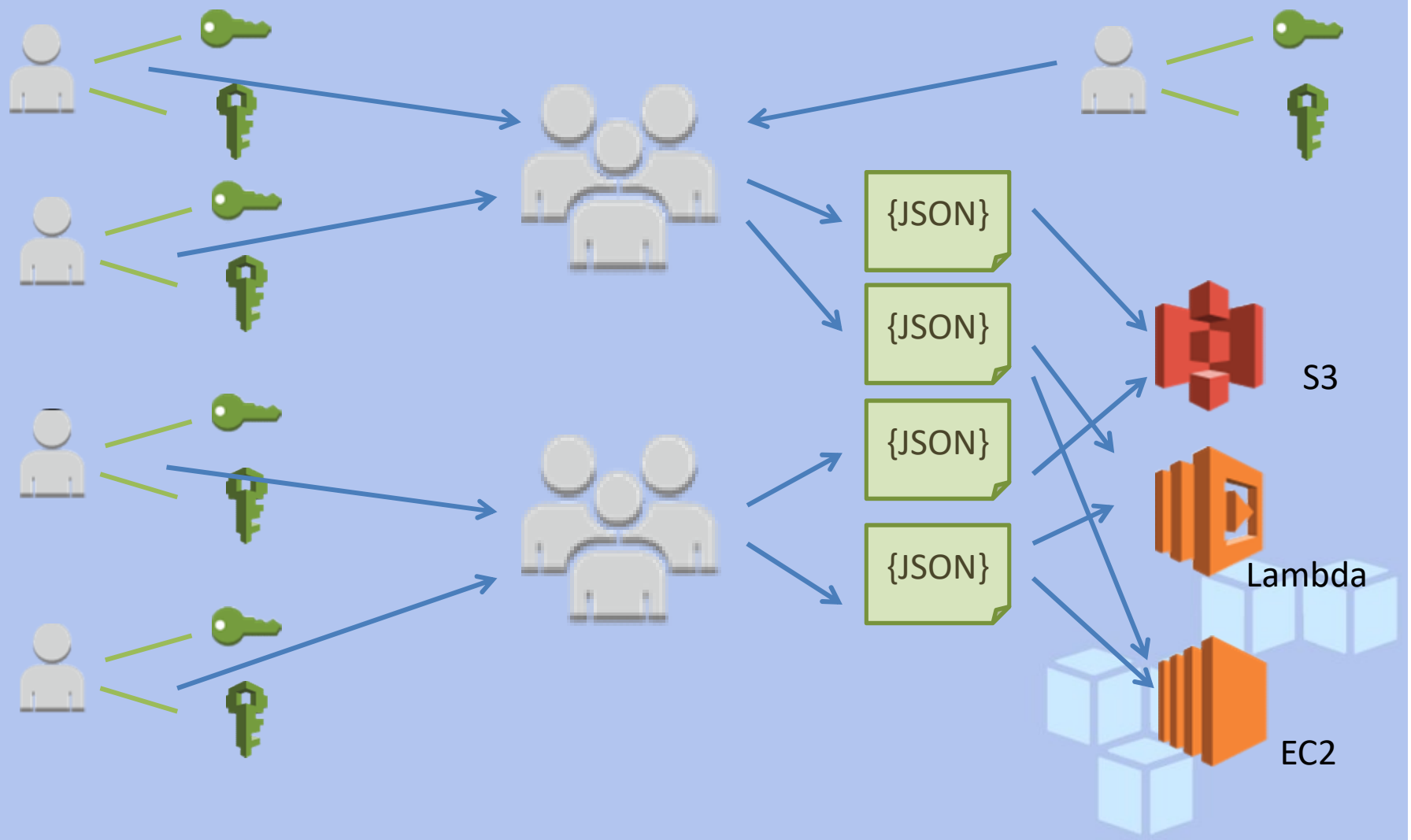
MzIzNzJjMzJjM2UyOGY5YzNiZTdlNjBlYjdlZDQyOWNkZTUzNTI5N2UzYTljYzc0ZTg1NTRkOWI3MzIzNzJjMzJjM2UyOGY5YzN

Konto Root i MFA

- Konto główne
- Nie używamy Access Keys – usuwamy jeśli są
- Używamy MFA
- Używamy tylko w wyjątkowych sytuacjach



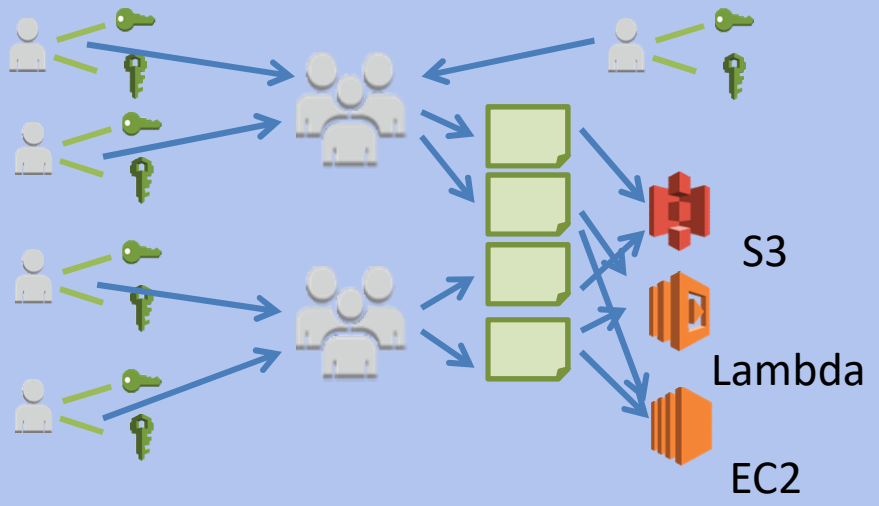
Jak powstaje chaos



Jak powstaje chaos

1 aplikacja na 1 koncie

- 2 dev 4 klucze
- 2 adm 4 klucze
- Konto tech 1 klucz



100 aplikacji na 10 kontach

- 20 dev 400 kluczy
- 10 adm 200 kluczy
- 100 kont tech 100 kluczy

700 kluczy, które mogą wyciec i które trzeba rotować

MzIzNzJjMzJjM2UyOGY5YzNiZTdlNjBlYjdlZDQyOWNkZTUzNTI5N2UzYTljYzc0ZTg1NTRkOWI3MzIzNzJjMzJjM2UyOGY5YzN

Jak powstaje chaos

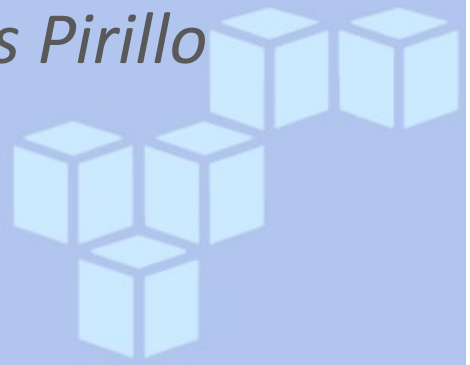
- Jeśli mamy w uprawnieniach „Deny” dla zasobów innej aplikacji to user nie może obsługiwać obu aplikacji jednym kontem. Powstają zależności między uprawnieniami.
- Każdy user ma wiele kont (na różnych kontach AWS), wiele kluczy
- Każda aplikacja ma innego usera i inny klucz

Czy to nie tylko paranoja „Bezpieczników”

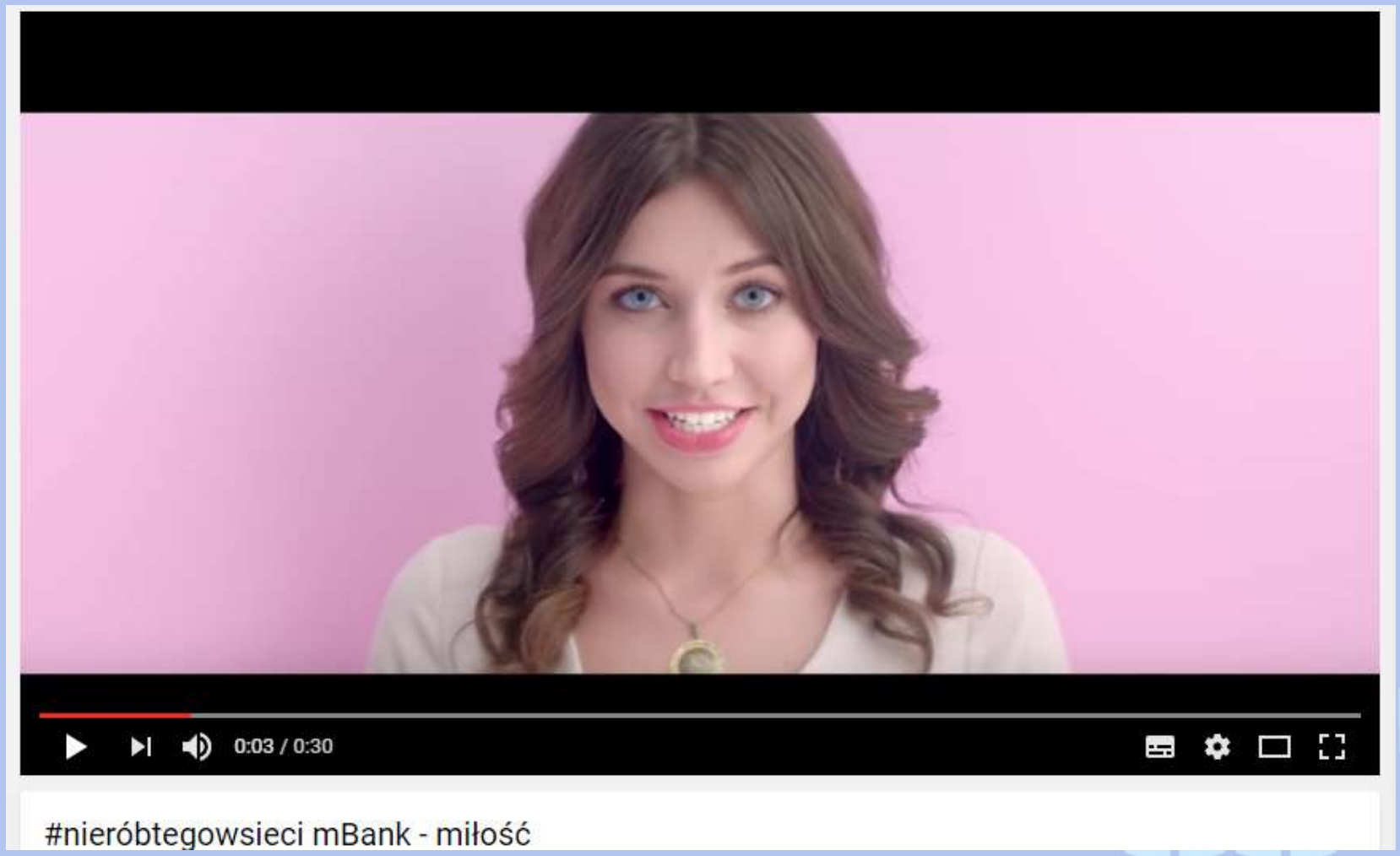
„Hasła są jak bielizna:

- *Nie pozwól żeby ludzie je widzieli*
- *Powinno się je często zmieniać*
- *Nie powinno się ich dzielić z obcymi”*

Chris Pirillo



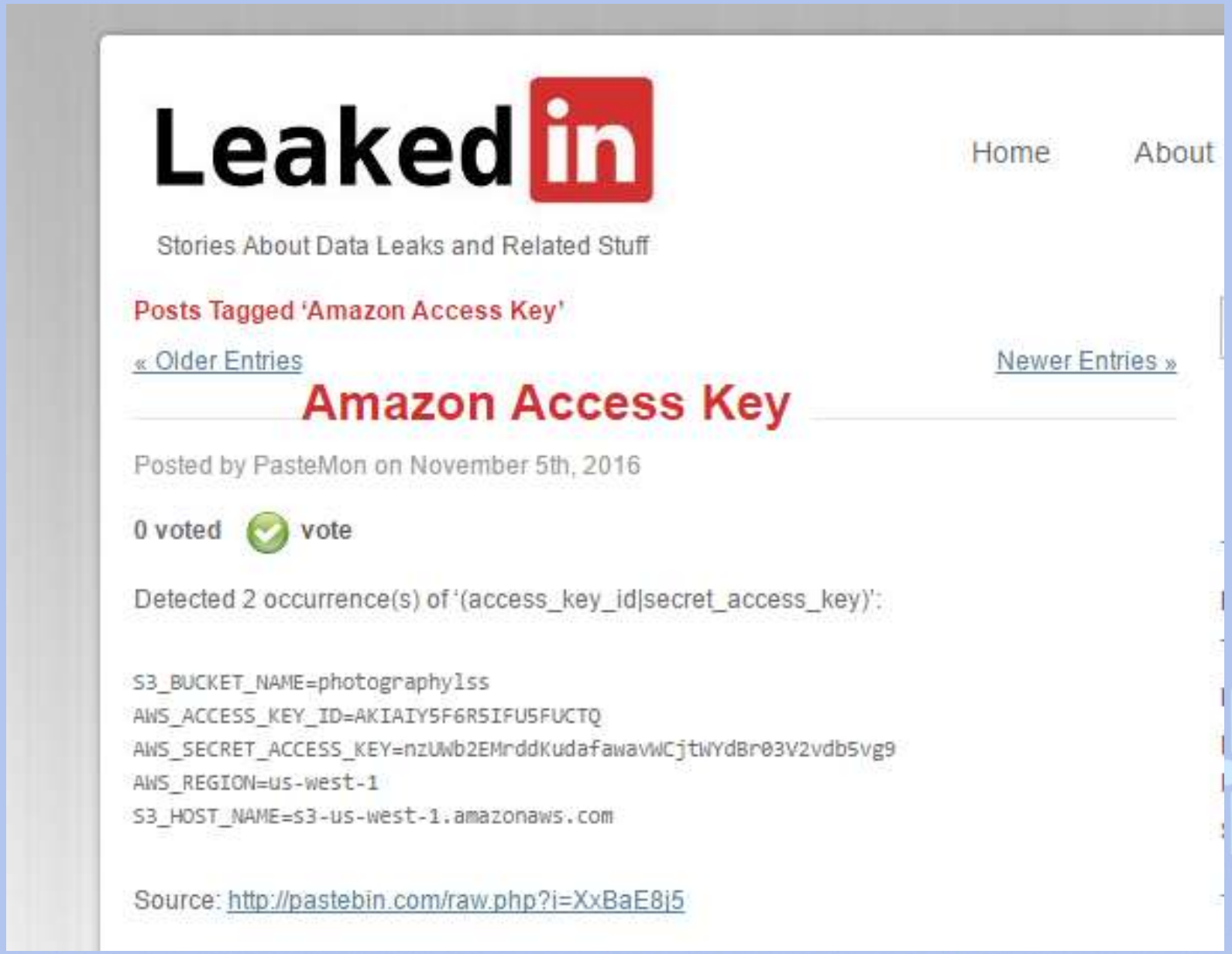
mBankTV



https://youtu.be/JpQa6415QPw

MzIzNzJjMzJjM2UyOGY5YzNiZTdlNjBlYjdlZDQyOWNkZTUzNTI5N2UzYTljYzc0ZTg1NTRkOWI3MzIzNzJjMzJjM2UyOGY5YzN

http://www.leakedin.com/tag/amazon-access-key/



Leaked in

Home About

Stories About Data Leaks and Related Stuff

Posts Tagged 'Amazon Access Key'

« Older Entries Newer Entries »

Amazon Access Key

Posted by PasteMon on November 5th, 2016

0 voted vote

Detected 2 occurrence(s) of '(access_key_id|secret_access_key)':

```
S3_BUCKET_NAME=photographylss
AWS_ACCESS_KEY_ID=AKIAIY5F6R5IFU5FUCTQ
AWS_SECRET_ACCESS_KEY=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
AWS_REGION=us-west-1
S3_HOST_NAME=s3-us-west-1.amazonaws.com
```

Source: http://pastebin.com/raw.php?i=XxBaE8j5

http://pastebin.com/raw/XxBaE8j5

https://sekurak.pl/

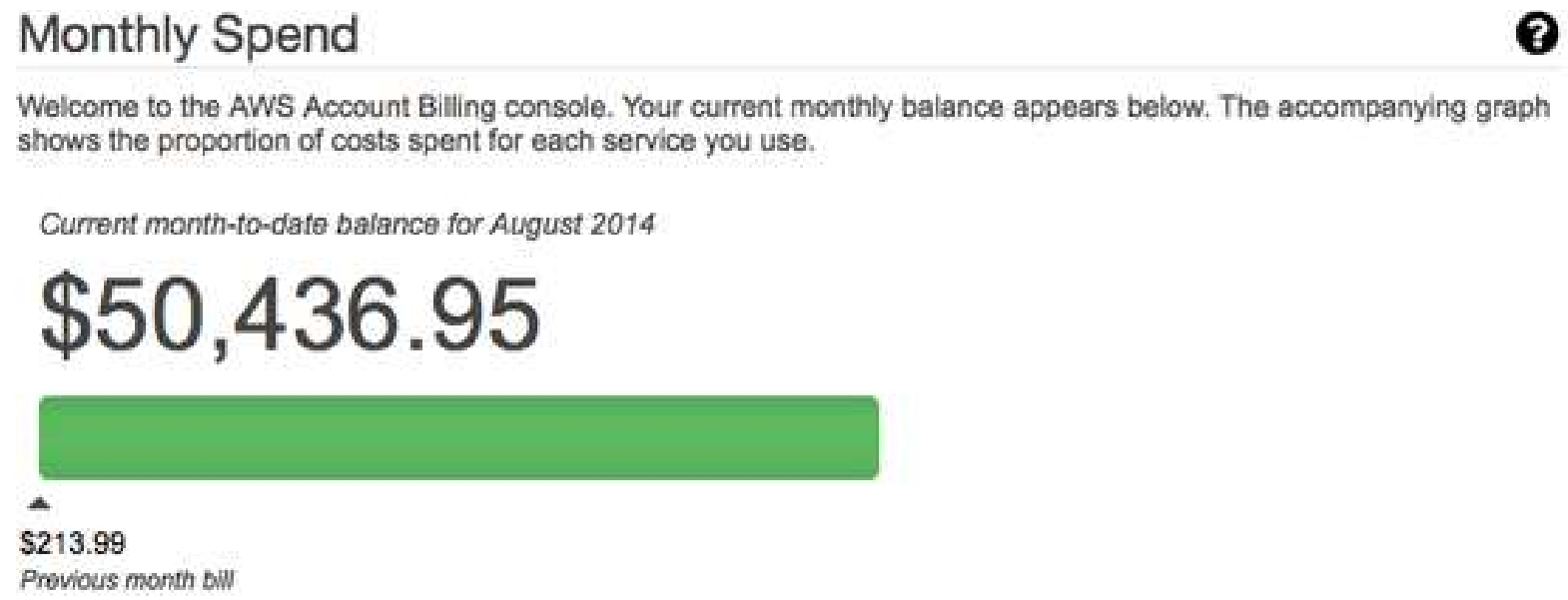
Ciekawe badanie oraz sam system do analizy aplikacji androidowych (potrafi analizować appki bezpośrednio z Google Play...):

Analiza polega na poszukiwaniu *zahardcodowanych* kluczy i innych interesujących ciągów znaków (haseł) w aplikacjach. Na ~16000 aplikacji znaleziono takich około 2500. Możecie zaprotestować, że nie wszystkie zapisane w appkach np. klucze API są groźne. I racja, tych problematycznych jest znacznie mniej – autorzy wpisu podali szacunek na około 304 aplikacji.

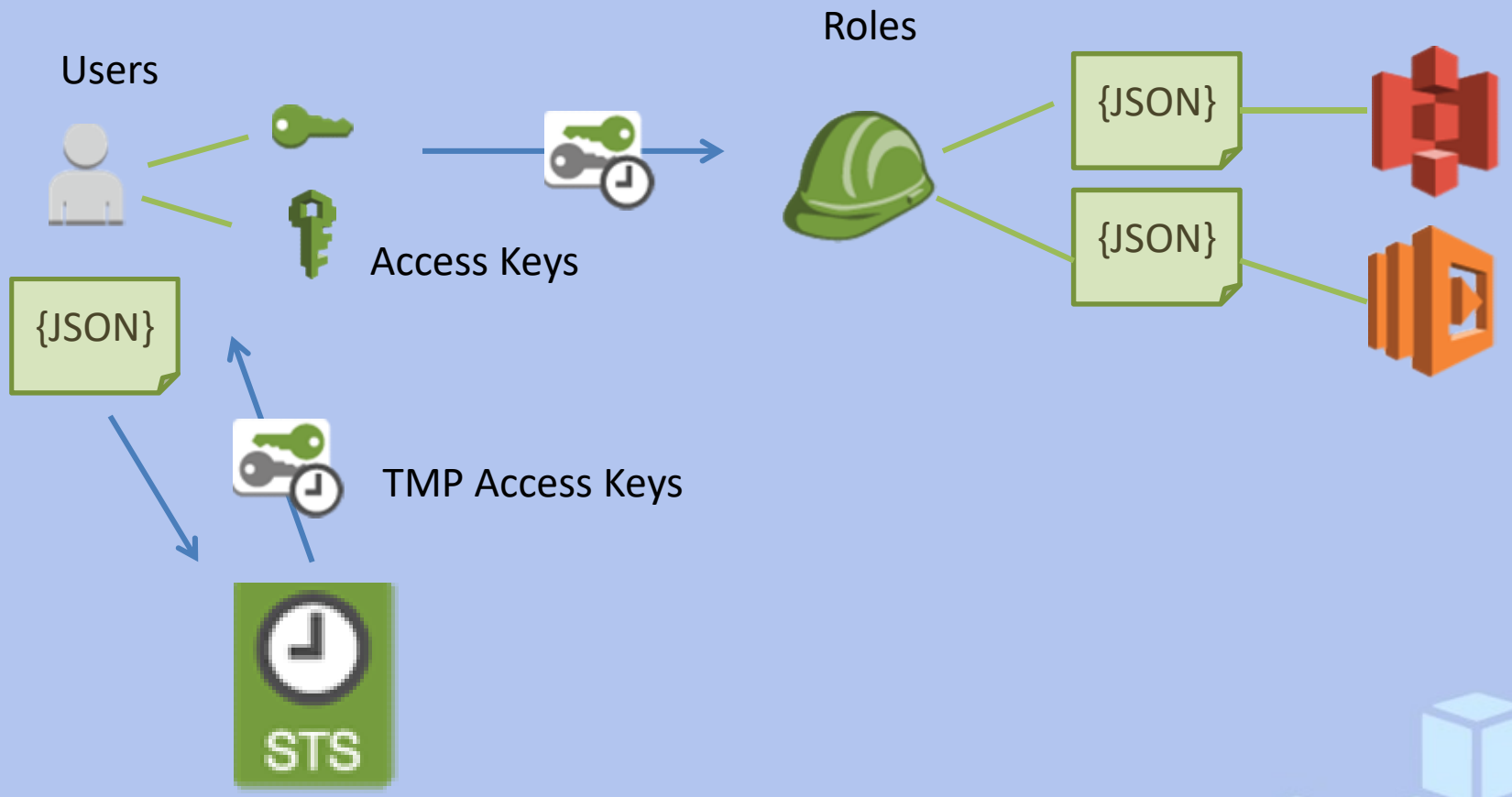
Przykład? Klucz do AWS dający pełne uprawnienia (umożliwiający np. tworzenie, usuwanie instancji):

My AWS account was hacked and I have a $50,000 bill, how can I reduce the amount I need to pay?

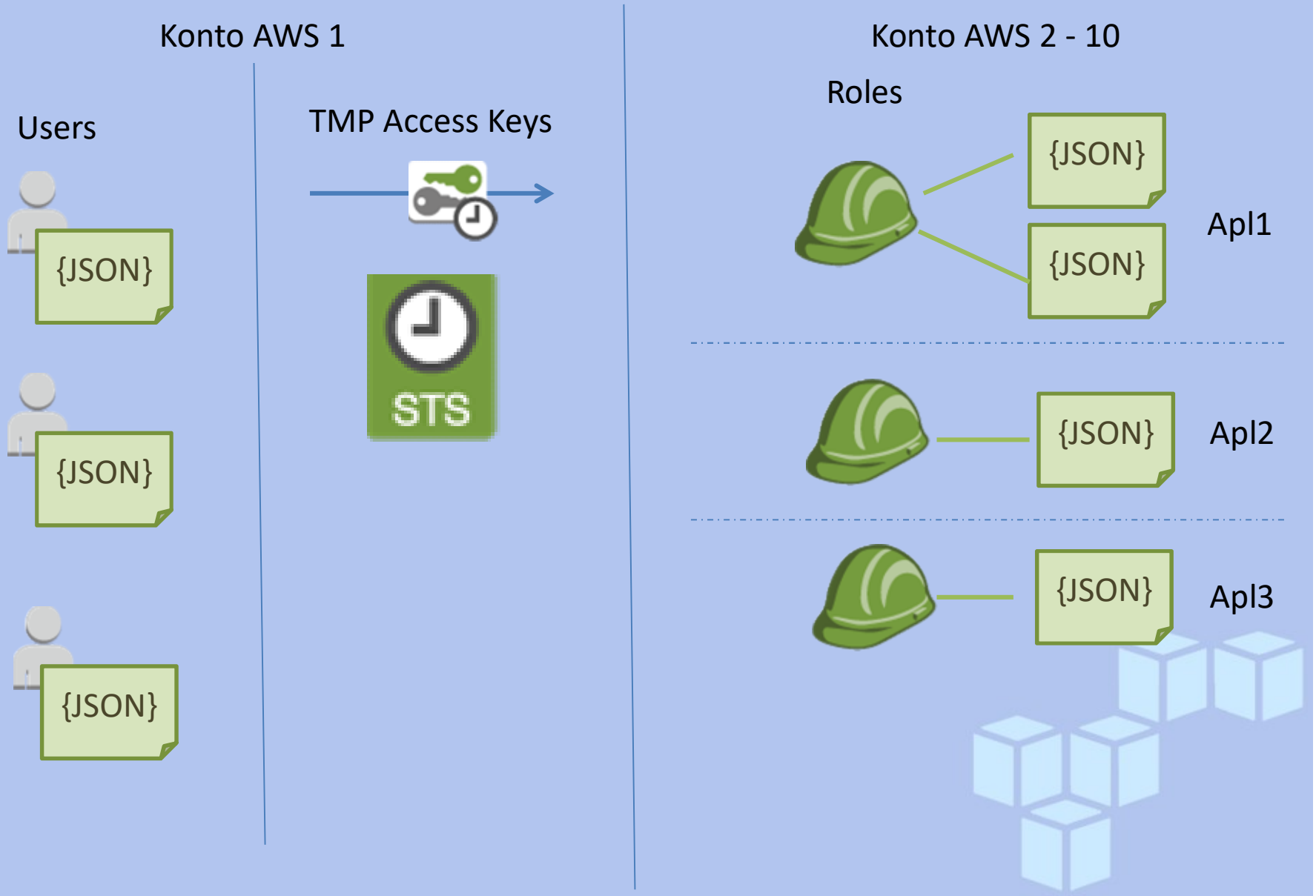
For years, my bill was never above $350/month on my single AWS instance. Then over the weekend someone got hold of my private key and launched hundreds of instances and racked up a $50,000 bill before I found out about it on Tuesday. Amazon had sent a warning by email at $15,000 saying they had found our key posted publicly, but I didn't see it. Naturally, this is a devastating amount of money to pay. I'm not saying I shouldn't pay anything, but this just a crazy amount in context. Amazon knew the account was compromised, that is why they sent an email, they knew the account history and I had only spent $213 the previous month. I almost feel they deliberately let it ride to try to earn more money. Does anyone have any experience with this sort of problem?



Uprawnienia kolejne starcie



Uprawnienia kolejne starcie



Uprawnienia kolejne starcie

Aplikacja

```
import boto3

session = boto3.Session(profile_name='tajnepliki')
s3 = session.resource('s3')
bucket = s3.Bucket('tajne')
obj = bucket.Object('superTajny.zip')
obj.download_file('/tmp/tmp.zip')
```

Profil

~/.aws/config

```
[profile tajnepliki]
region = eu-central-1
role_arn=arn:aws:iam::98675345:role/s3Ap1
source_profile=rotowany
```

Access Keys

~/.aws/credentials

```
[rotowany]
aws_access_key_id = AKI.....
aws_secret_access_key = Ujtcc9J4AC.....
```

Czy coś zyskaliśmy ?

- Niezależne zbiory uprawnień
- Separacje aplikacji od profili i łatwy sposób na rotowanie kluczy
- System odporniejszy na kompromitacje dostępów
- Łatwe zarządzanie użytkownikami, tylko na jednym koncie
- Możliwość działania w kontekście aplikacji
- Przejrzystą strukture