Adobe's Security Blunder

Celso Celante
Thuy Nguyen
Lucilia Oliveira

Security

Adobe pays US$1.2M plus settlements to end 2013 breach class action

Popped Photoshop factory happy to see court case end.

17 Aug 2015 at 06:58, Darren Pauli

ADOBE NEWS

IMPORTANT CUSTOMER SECURITY ANNOUNCEMENT

POSTED BY BRAD ARKIN, CHIEF SECURITY OFFICER ON OCTOBER 3, 2013

Cyber attacks are one of the unfortunate realities of doing business today. Given the profile and widespread use of many of our products, Adobe has attracted increasing attention from cyber attackers. Very recently, Adobe's security team discovered sophisticated attacks on our network, involving the illegal access of customer information as well as source code for numerous Adobe products. We believe these attacks may be related.

Our investigation currently indicates that the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders.

What happened?

- Data breach of 38 million users

- Hackers raided a backup server

- Shoddy security protocols

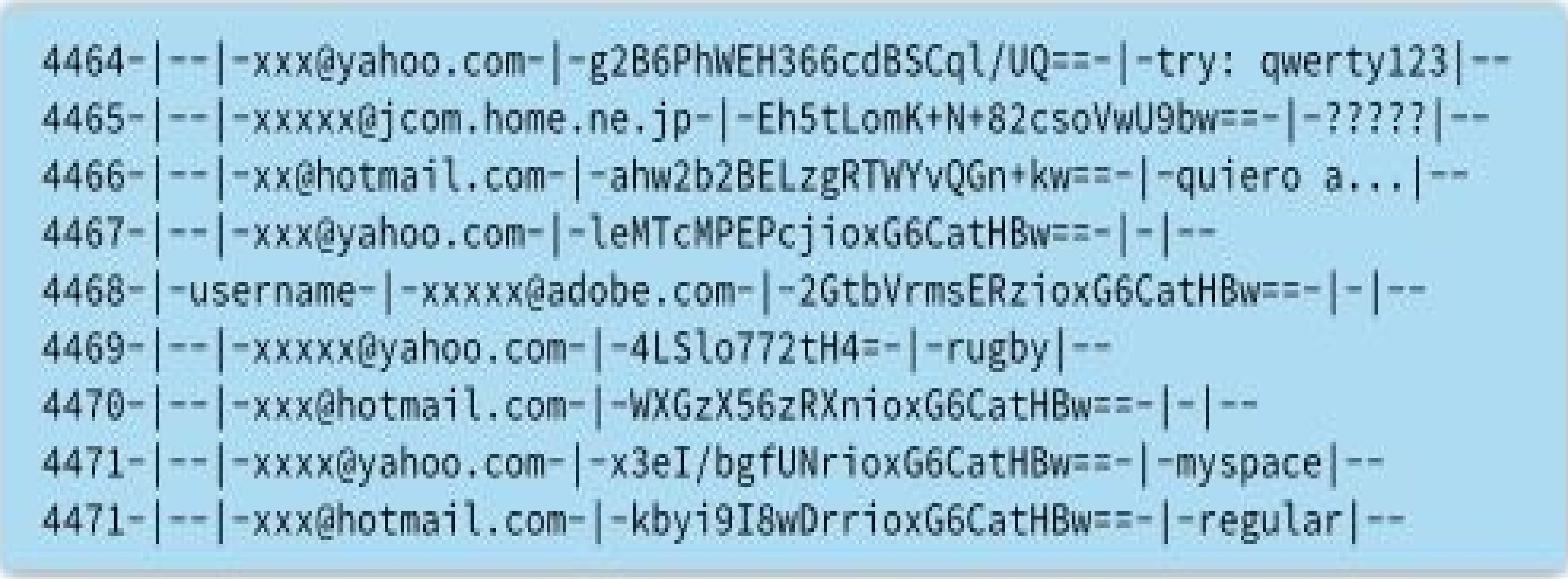
```
function
  var wW = 0;
  if (typeof window.innerWidth
    wW = window.innerWidth;
  } else if (document.documentElement && docum
    wW = document.documentElement.clientWid
  } else if (document.body && document.body.c
    wW = document.body.clientWidth;
  }
  if (sH = document.documentElement.scrollH
  var wH = window.innerHeight || docume
  var sW = !document.all && (sH > wH)
      (getStyle('menu', 'wid
      W)) {
```

What was stolen?

- 3.8 GB files
  - Customers’ credit card numbers
  - 152 million usernames
  - Poorly-encrypted passwords

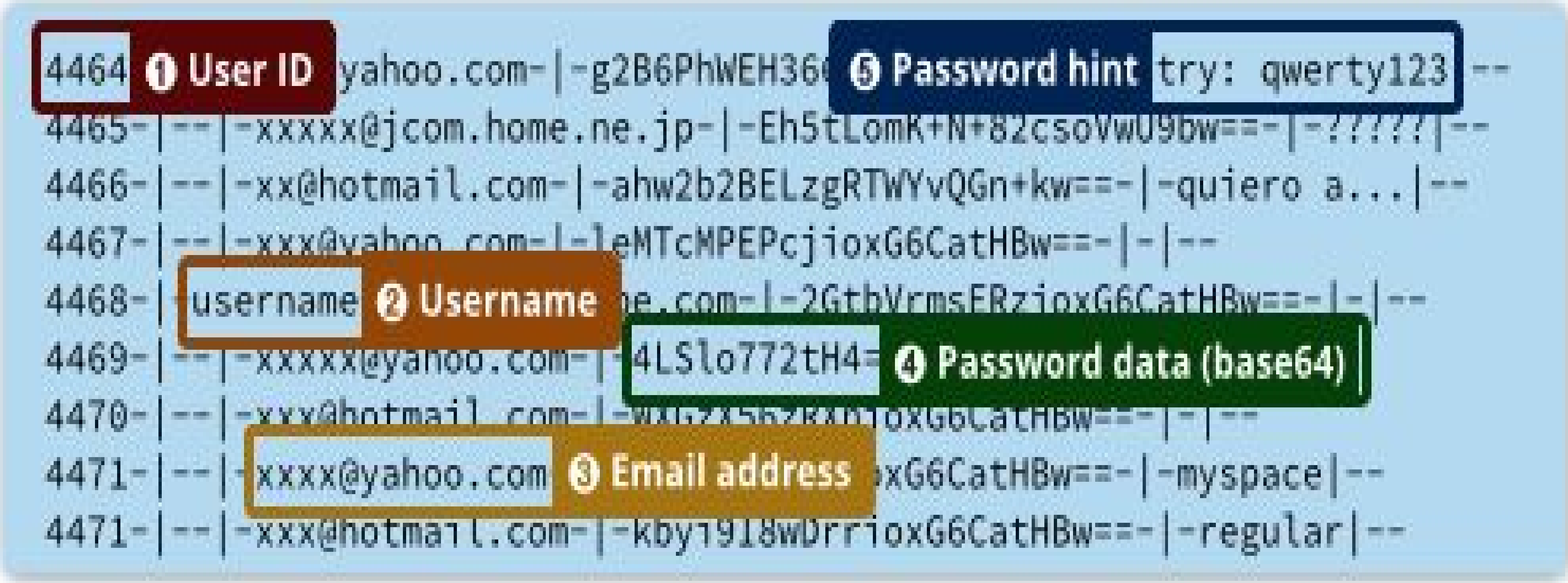
- Other files with sources codes for
  - Adobe Photoshop, Acrobat, Reader, and Cold Fusion

User’s Database Dump



```
4464-|--|-xxx@yahoo.com-|-g2B6PhWEH366cdBSCql/UQ==-|-try: qwerty123|--
4465-|--|-xxxxx@jcom.home.ne.jp-|-Eh5tLomK+N+82csoVwU9bw==-|-?????|--
4466-|--|-xx@hotmail.com-|-ahw2b2BELzgRTWYvQGn+kw==-|-quiero a...|--
4467-|--|-xxx@yahoo.com-|-leMTcMPEPcjioxG6CatHBw==-|-|--
4468-|-username-|-xxxxx@adobe.com-|-2GtbVrmsERzioxG6CatHBw==-|-|--
4469-|--|-xxxxx@yahoo.com-|-4LSlo772tH4=-|-rugby|--
4470-|--|-xxx@hotmail.com-|-WXGzX56zRXnioxG6CatHBw==-|-|--
4471-|--|-xxxx@yahoo.com-|-x3eI/bgfUNrioxG6CatHBw==-|-myspace|--
4471-|--|-xxx@hotmail.com-|-kbyi9I8wDrrioxG6CatHBw==-|-regular|--
```

User’s Database Dump



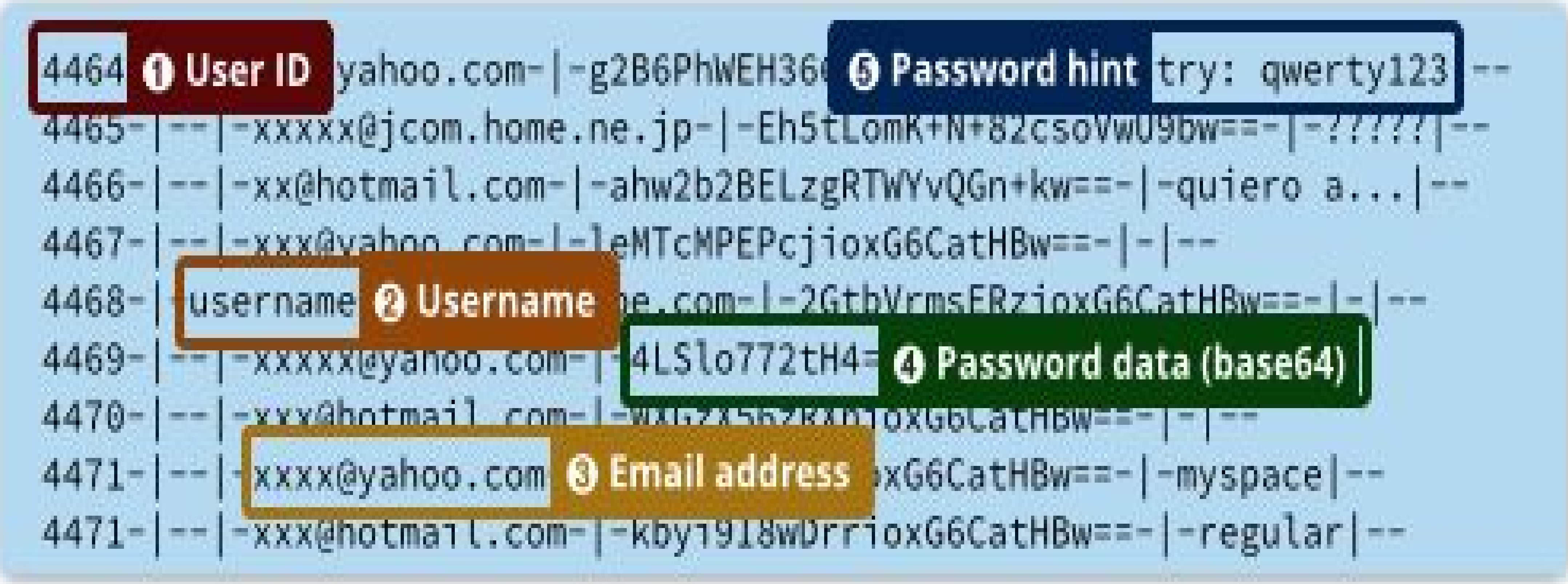
```
4464 yahoo.com-|-g2B6PhWEH36 try: qwerty123|--
4465-|--|-xxxxx@jcom.home.ne.jp-|-Eh5tLomK+N+82csoVwU9bw==-|-?????|--
4466-|--|-xx@hotmail.com-|-ahw2b2BELzgRTWYvQGn+kw==-|-quiero a...|--
4467-|--|-xxx@yahoo.com-|-leMTcMPEPcjioxG6CatHBw==-|-|--
4468-|-username e.com-|-2GtbVrmsERzioxG6CatHBw==-|-|--
4469-|--|-xxxxx@yahoo.com-|-4LSlo772tH4=
4470-|--|-xxx@hotmail.com-|-WXGZX562RXDioxG6CatHBw==-|-|--
4471-|--|-xxxx@yahoo.com xG6CatHBw==-|-myspace|--
4471-|--|-xxx@hotmail.com-|-kbyi918wDrrioxG6CatHBw==-|-regular|--
```

The Security Breach

Main Issues

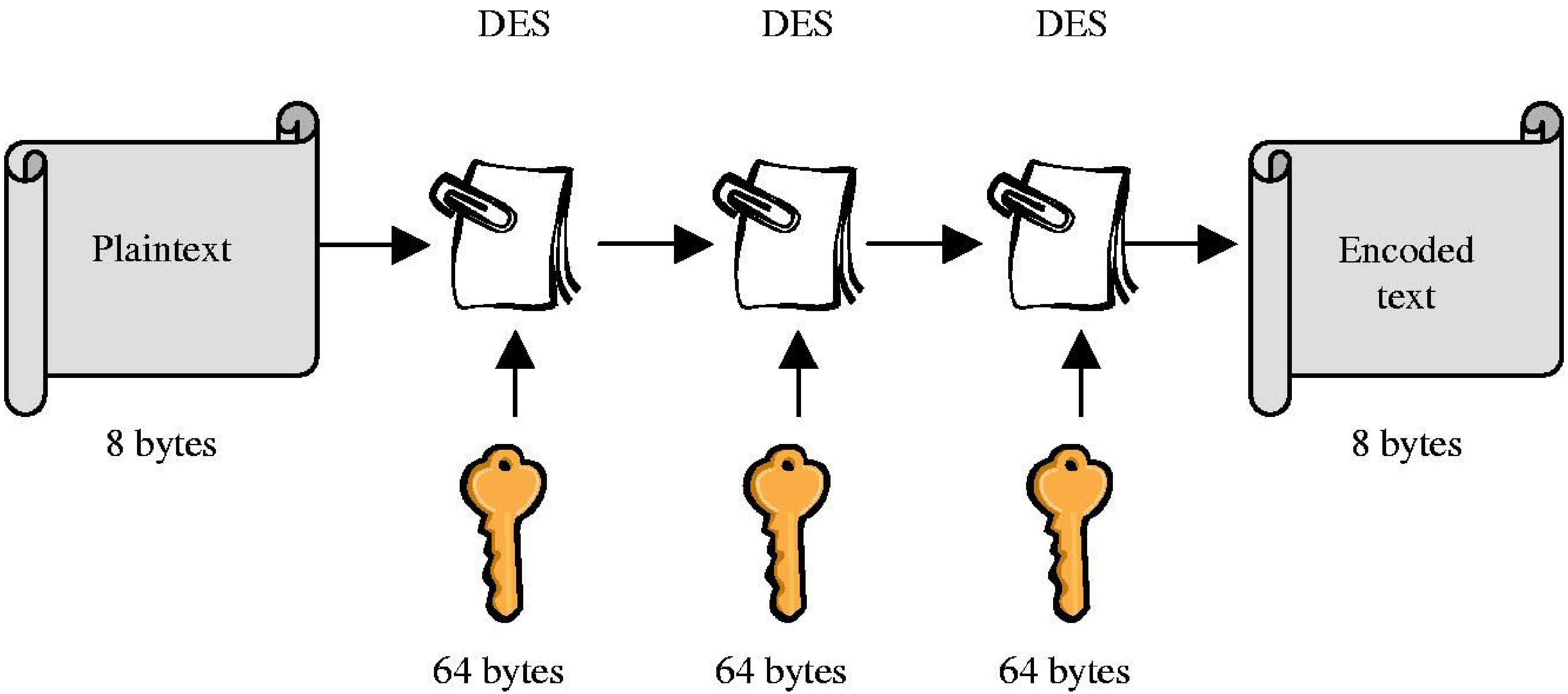
- **Hints**: Password hints were not encrypted.
- **Reversible**: Possible to recover the passwords.
- **Same key**: Allows the hacker to recover all the passwords.

User’s Database Dump



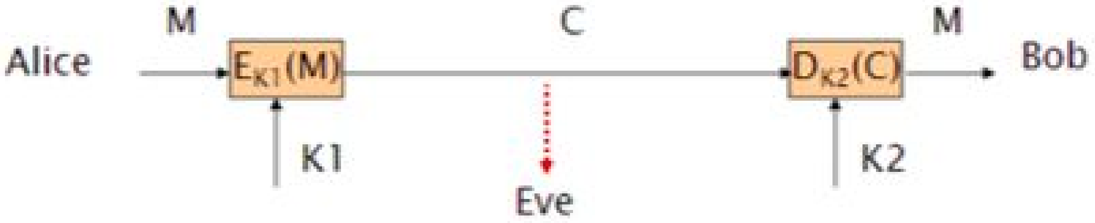
```
4464               yahoo.com-|-g2B6PhWEH36                       try: qwerty123 |--
4465-|--|-xxxxx@jcom.home.ne.jp-|-Eh5tLomK+N+82csoVwU9bw==-|-?????|--
4466-|--|-xx@hotmail.com-|-ahw2b2BELzgRTWYvQGn+kw==-|-quiero a...|--
4467-|--|-xxx@yahoo.com-|-leMTcMPEPcjioxG6CatHBw==-|-|--
4468-|-username                 e.com-|-2GtbVrmsERzioxG6CatHBw==-|-|--
4469-|--|-xxxxx@yahoo.com-|-4LSlo772tH4=
4470-|--|-xxx@hotmail.com-|-wxGzx562RxDioxG6CatHBw==-|-|--
4471-|--|-xxxx@yahoo.com                    xG6CatHBw==-|-myspace|--
4471-|--|-xxx@hotmail.com-|-kby1918wDrrioxG6CatHBw==-|-regular|--
```

Triple DES (3DES) Algorithm

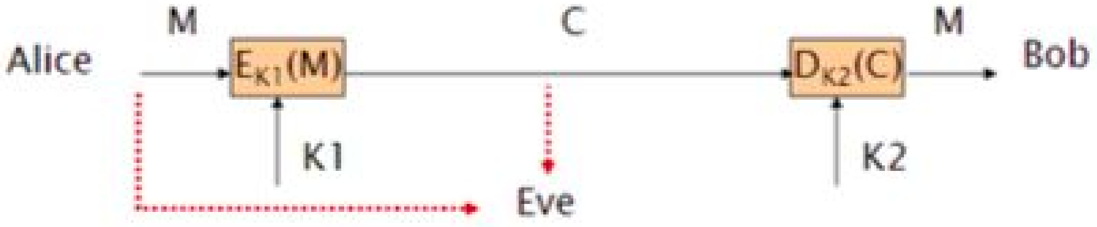


Types of Attack

Ciphertext-only attack



Known-plaintext attack

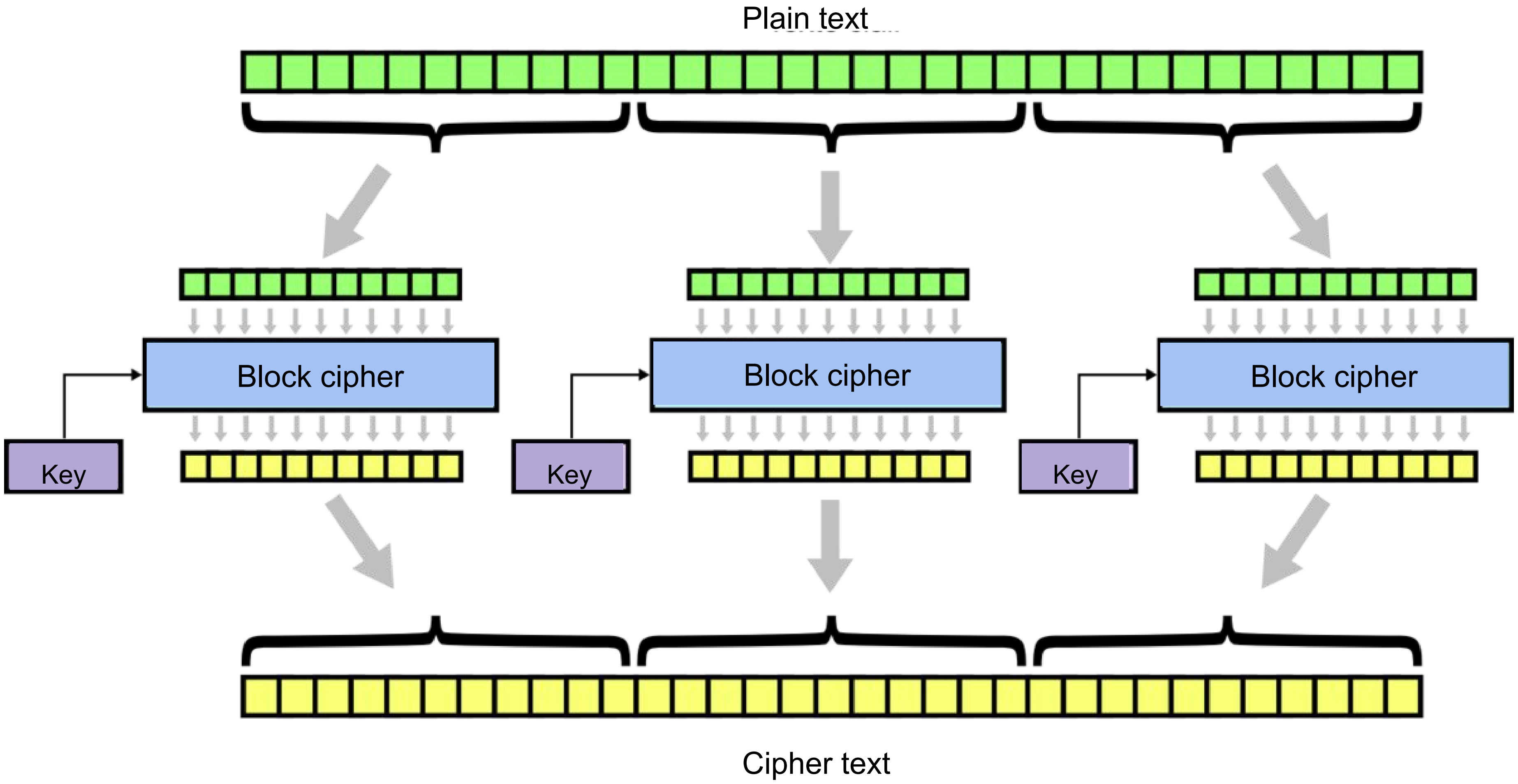


Electronic Code Book (ECB)

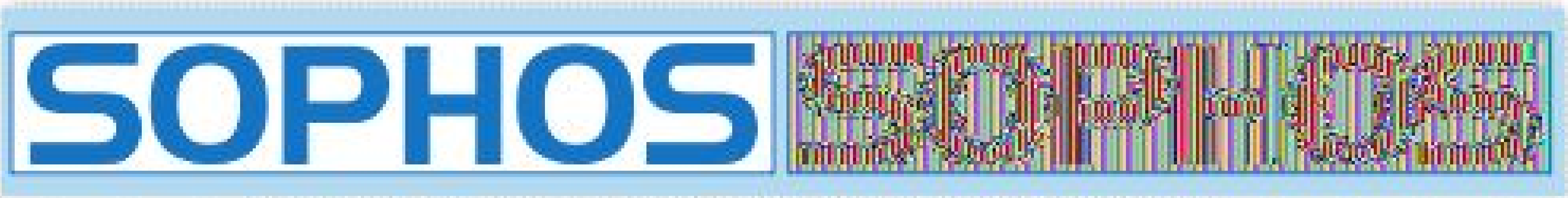
- The message is **divided into blocks**, and each block is encrypted separately.

- **Identical plaintext** blocks are encrypted to **identical ciphertext** blocks.
  - ECB does not provide enough confidentiality.

Electronic Code Book (ECB)



Electronic Code Book (ECB)



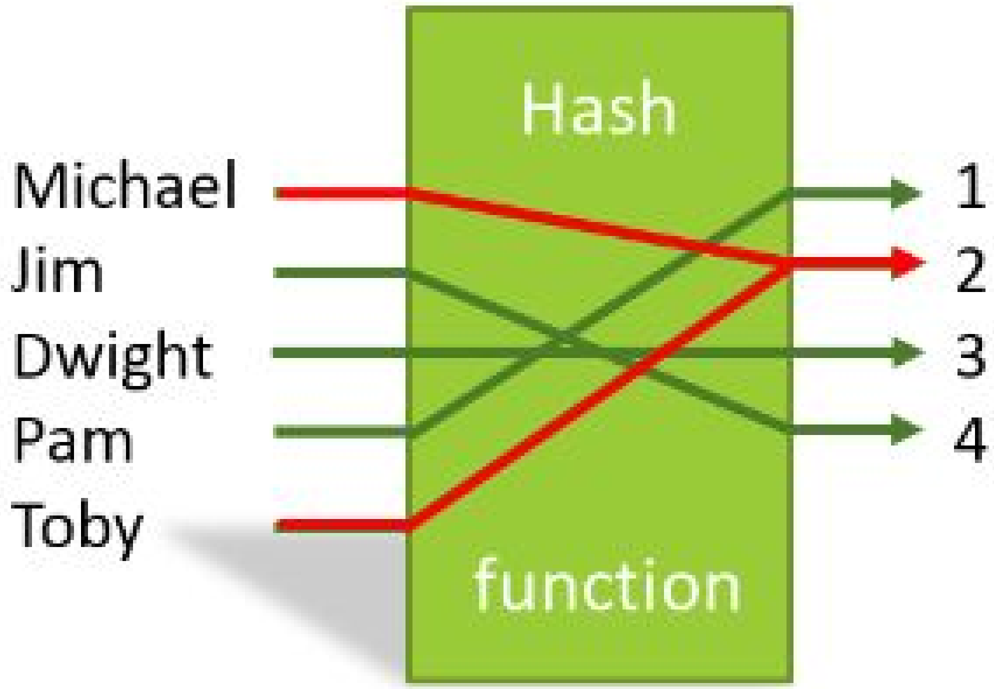
Left: Sophos logo as regular RGB (3-bytes-per-pixel) file

Right: Same file enrypted 8 bytes at a time using ECB mode

A Possible Solution

What is hashing?

- **Hashing** is the transformation of a string into a usually unique fixed-length value or key using a hash function.



What makes hashing suitable for protecting password?

- **Hash function is one way**: No algorithm to go back to password string from the hash string

- **Each hash always hash to the same thing**: Password can be compared since only one function is used to do hashing

- **Different hash string for very similar password**: Great for protecting

Example

hash("hello") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1f

hash("hbllo") = 58756879c05c68dfac9866712fad6a93f8146f337a6

hash(“hellz") = 81794384491161f1777c232bc6bd9ec38f616560b12

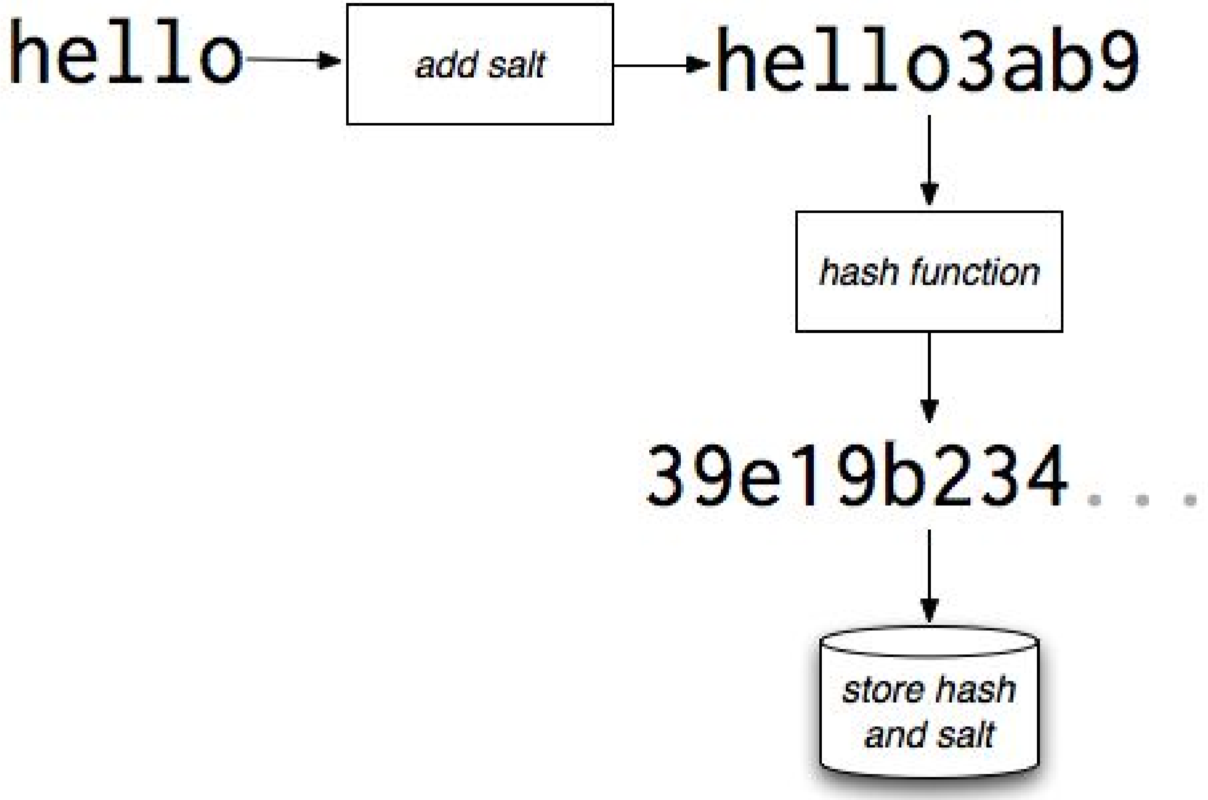
Hashing with Salt

- **What is salt**: A salt is simply added to make a common password uncommon

- **Increases security level**: We can randomize the password by adding arbitrary string (salt) to the password.

How salt works

We stored the **hashed string** and the **salt** together in the user account database



Notice when using salt

- **Salt reuse:** Common mistake is to use the same salt in each hash.
- **Short salt:** Attackers can look up table for every possible salt.

Questions

What types of attack are present?

Why is the use of short salts not recommended?

Which C.I.A. principle(s) does Electronic Code Block (ECB) break?

Questions

What types of attack are present?

A mix of ciphertext only and known plaintext.

Why is the use of short salts not recommended?

Once the set of possible salts is small, the attacker might try all the possibilities within considerable short amount of time.

Which C.I.A. principle(s) does Electronic Code Block (ECB) break?

Confidentiality.

References

- "Computer Security: Principles and Practice", W. Stallings, L. Brown, Pearson Education, 2014, 3rd Edition.
- http://www.theregister.co.uk/2015/08/17/adobe_settles_claims_for_data_breach/
- http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html
- http://www.courthousenews.com/2015/08/14/adobe-settles-claims-for-massive-data-breach.htm
- https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/
- http://www.csoonline.com/article/2134124/network-security/adobe-confirms-stolen-passwords-were-encrypted-not-hashed.html