CSE 490K Lecture 11

Crypto Details + Security Evaluation

Tadayoshi Kohno

Midterm

- Common security goals
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
- Threats, vulnerabilities
- Software security
  - Like Project 1
  - Buffer overflows
  - Format string vulnerabilities
  - Double-free bugs

Authentication & Usability

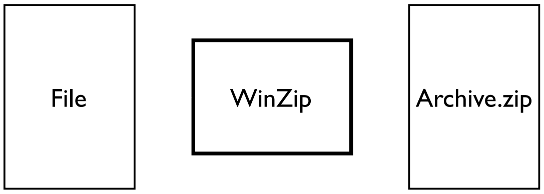
- Password strength
- Party-in-the-middle attacks
- Usability challenges

Midterm

- Crypto
  - Symmetric and Asymmetric (Know differences)
  - Encryption and Authenticated Encryption
  - Message Authentication
  - Block ciphers
  - Hash functions
  - PKIs
  - For all of the above:
    - What they are from an external perspective, not the internals (except for the one-time pad)
    - (No number theory, etc)
    - But be able to understand attacks, like the last homework assignment, Security Evaluation #2, and some stuff I'll show on the board

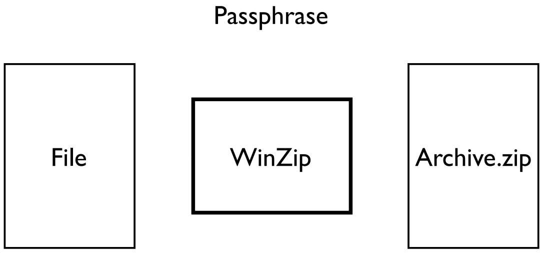
Security Evaluation

Very popular Windows compression utility. Also an Outlook email plugin. Over 160 million downloads from download.com alone [http://www.winzip.com/empopp.htm].

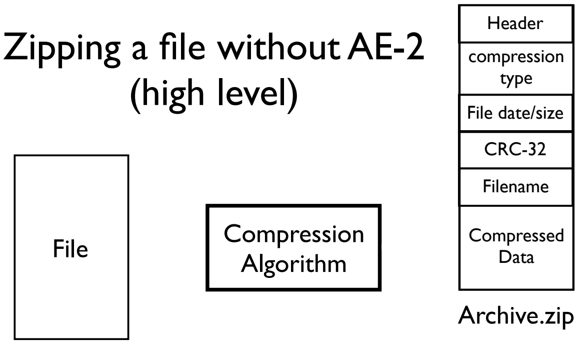


WinZip encryption

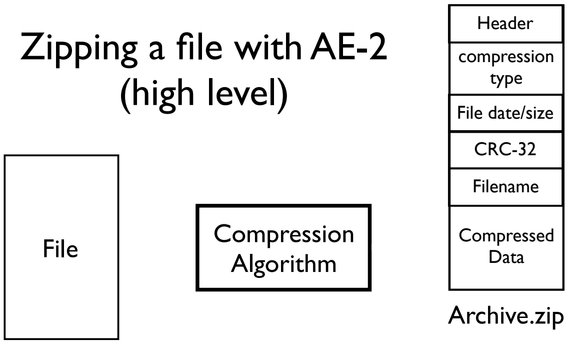
WinZip has the ability to encrypt files. Lots of history, but we'll look at the AE-2 method.



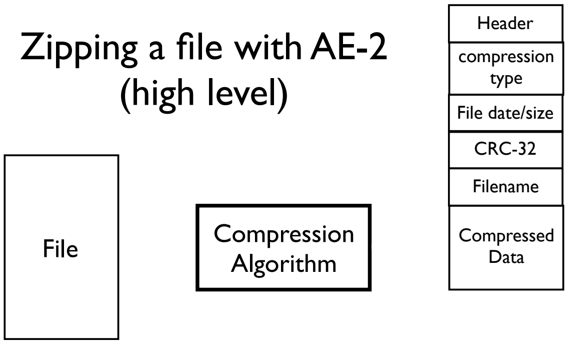
Zipping a file without AE-2 (high level)



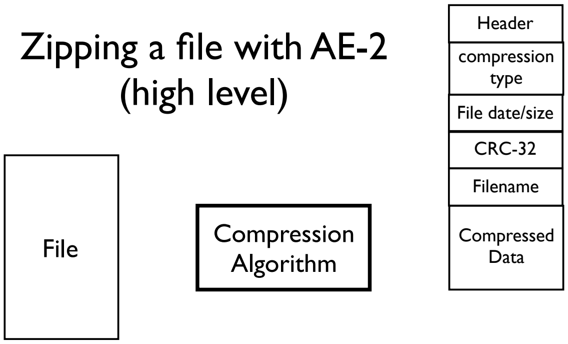
Zipping a file with AE-2 (high level)



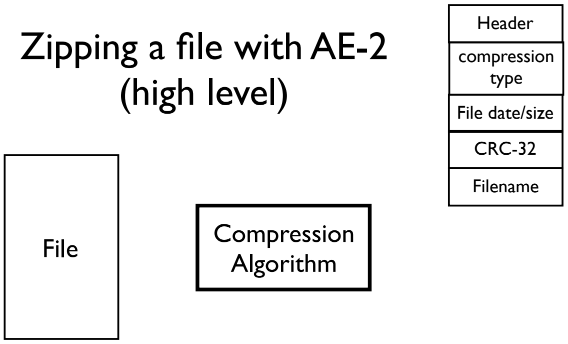
Zipping a file with AE-2 (high level)



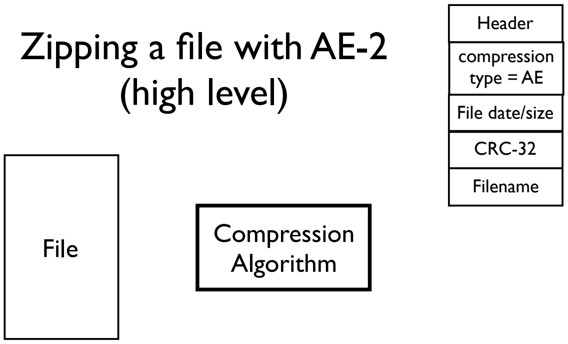
Zipping a file with AE-2 (high level)

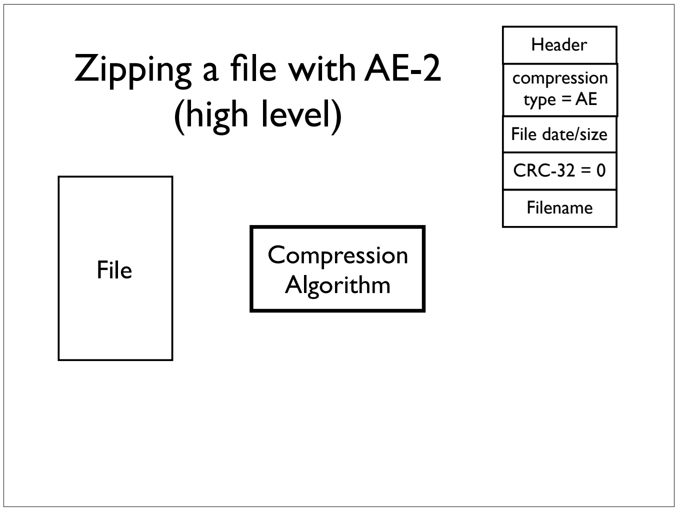


Zipping a file with AE-2 (high level)



Zipping a file with AE-2 (high level)



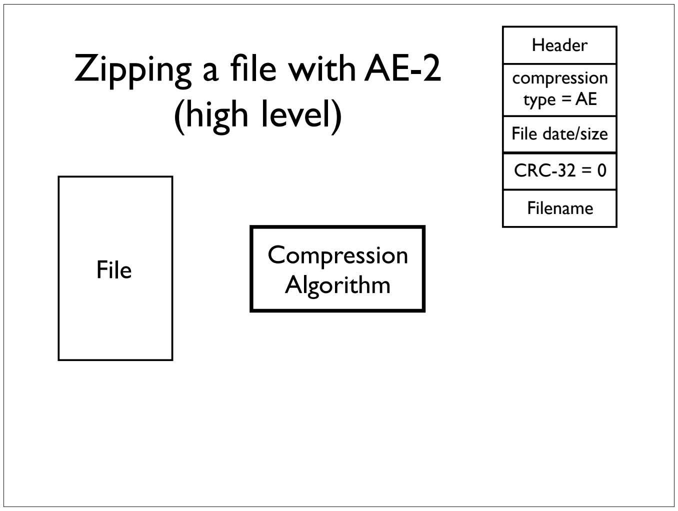


Zipping a file with AE-2 (high level)

Header
compression type = AE
File date/size
CRC-32 = 0
Filename

File

Compression Algorithm

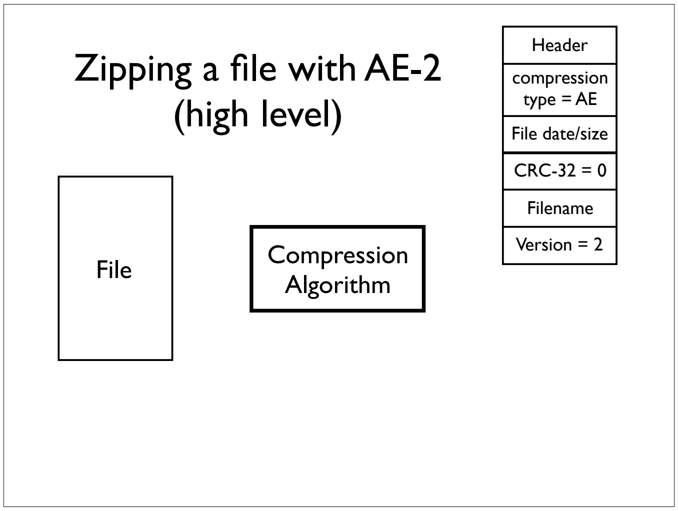


Zipping a file with AE-2 (high level)

Header
compression type = AE
File date/size
CRC-32 = 0
Filename

File

Compression Algorithm

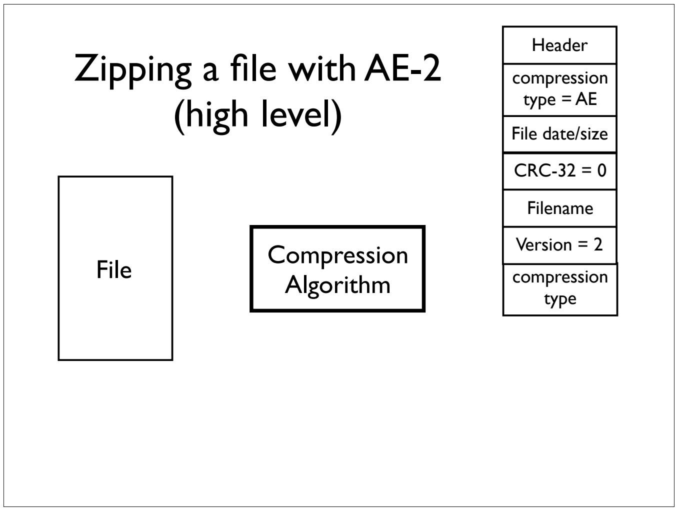


Zipping a file with AE-2 (high level)

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2

File

Compression Algorithm

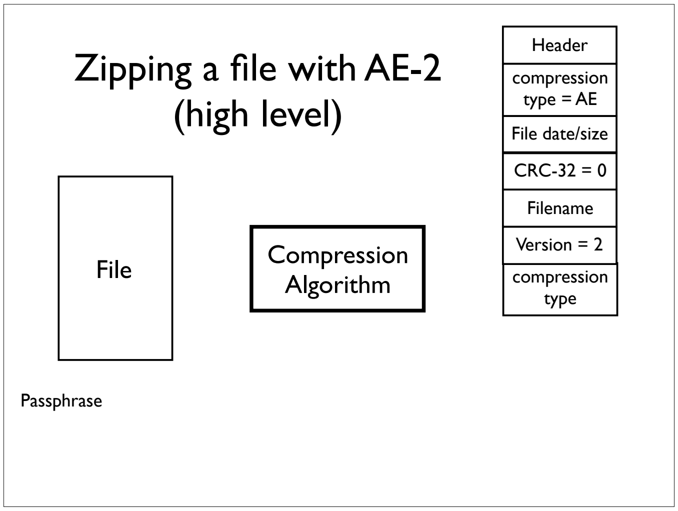


Zipping a file with AE-2 (high level)

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type

File

Compression Algorithm



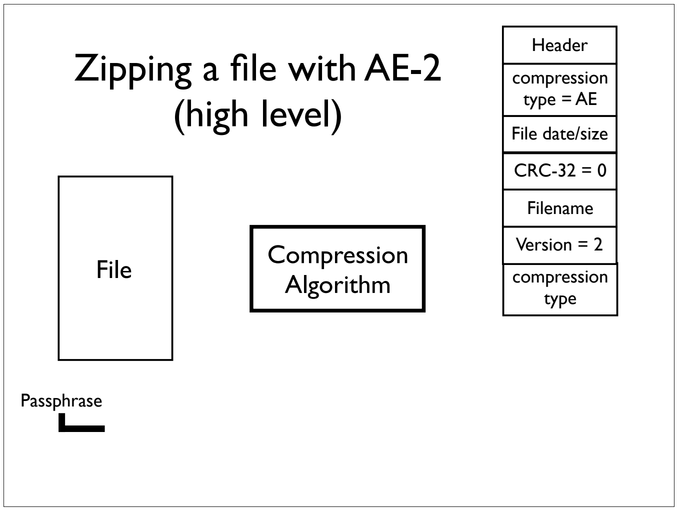
Zipping a file with AE-2 (high level)

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type

File

Compression Algorithm

Passphrase



Zipping a file with AE-2 (high level)

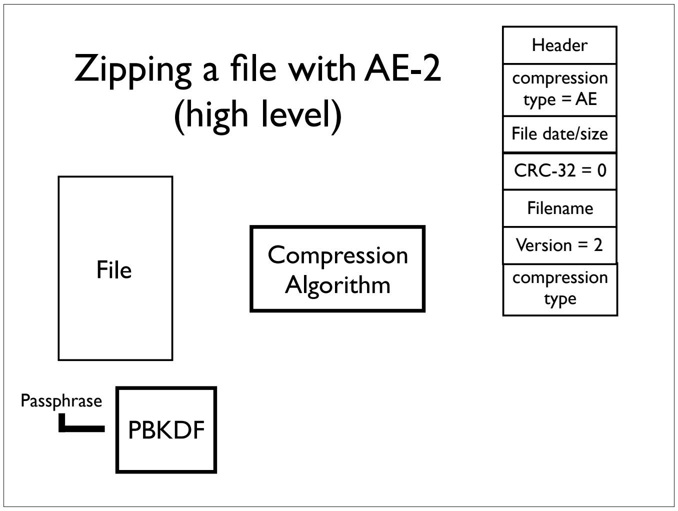
Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type

File

Compression Algorithm

Passphrase

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

Header

compression type = AE

File date/size

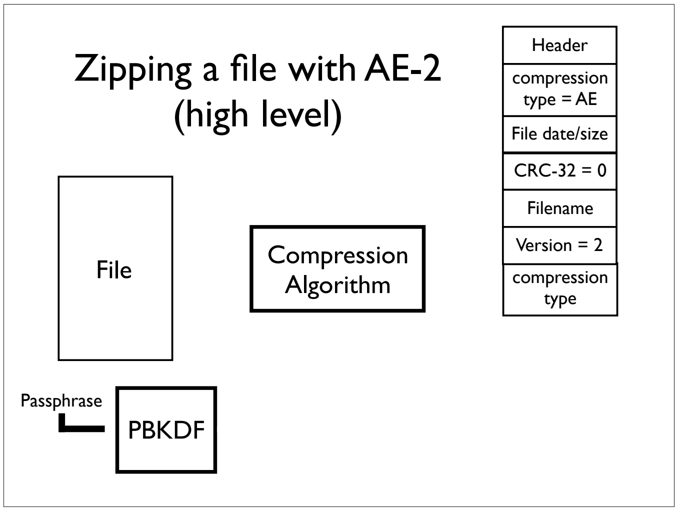
CRC-32 = 0

Filename

Version = 2

compression type

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

Header

compression type = AE

File date/size

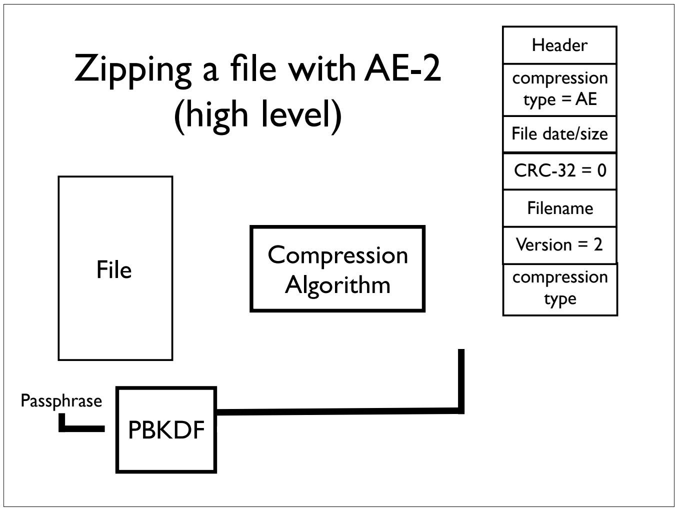
CRC-32 = 0

Filename

Version = 2

compression type

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

Header

compression type = AE

File date/size

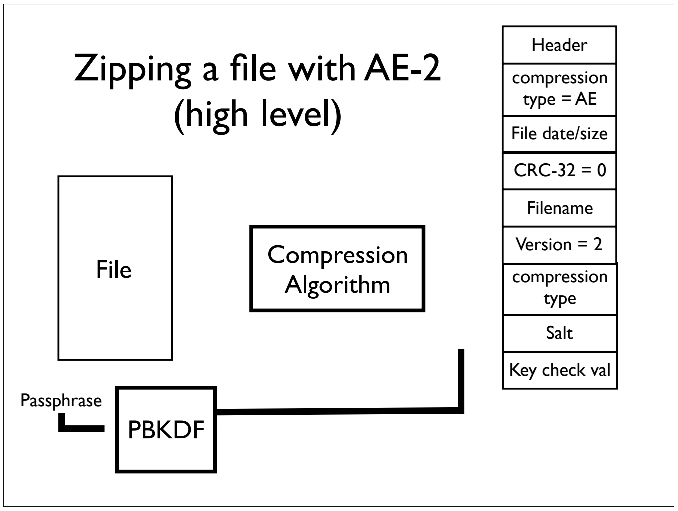
CRC-32 = 0

Filename

Version = 2

compression type

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

Header

compression type = AE

File date/size

CRC-32 = 0

Filename

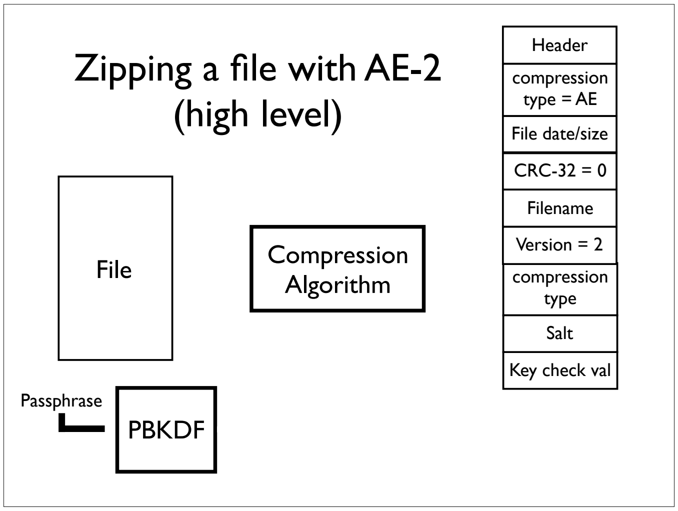
Version = 2

compression type

Salt

Key check val

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

Header

compression type = AE

File date/size

CRC-32 = 0

Filename

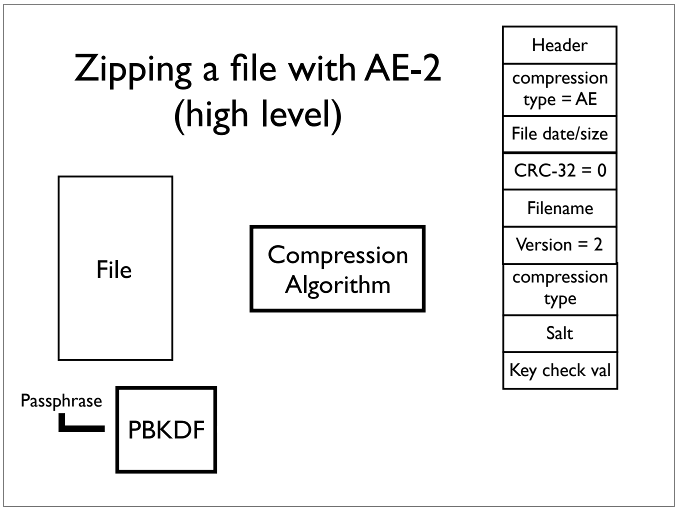
Version = 2

compression type

Salt

Key check val

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

Header

compression type = AE

File date/size

CRC-32 = 0

Filename

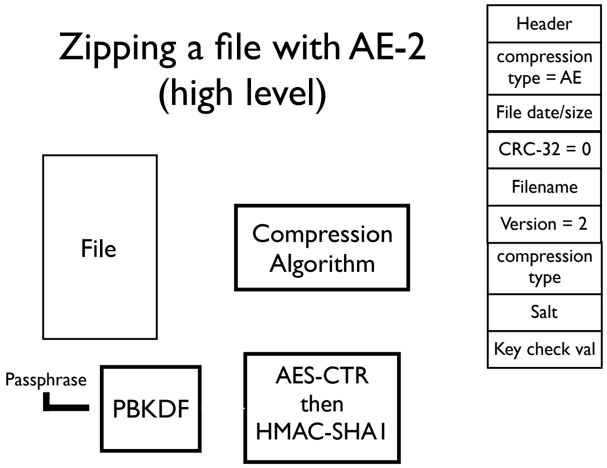
Version = 2

compression type

Salt

Key check val

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

AES-CTR then HMAC-SHA1

Header

compression type = AE

File date/size

CRC-32 = 0

Filename

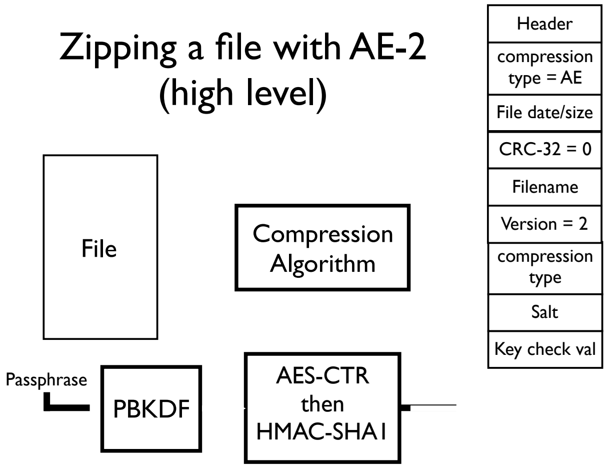
Version = 2

compression type

Salt

Key check val

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

AES-CTR then HMAC-SHA1

Header

compression type = AE

File date/size

CRC-32 = 0

Filename

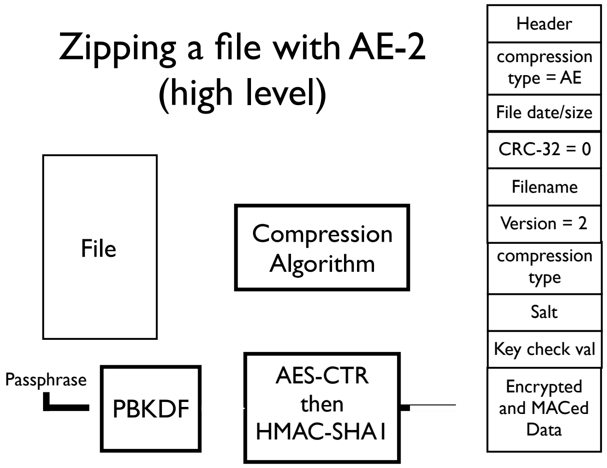
Version = 2

compression type

Salt

Key check val

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

AES-CTR then HMAC-SHA1

Header

compression type = AE

File date/size

CRC-32 = 0

Filename

Version = 2

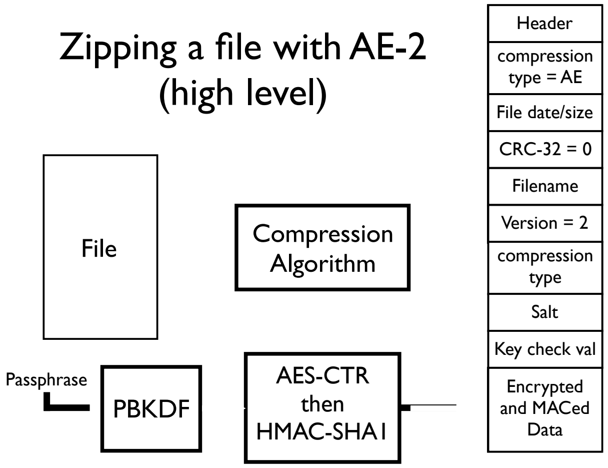
compression type

Salt

Key check val

Encrypted and MACed Data

Zipping a file with AE-2 (high level)



File

Compression Algorithm

Passphrase

PBKDF

AES-CTR then HMAC-SHA1

Header

compression type = AE

File date/size

CRC-32 = 0

Filename

Version = 2

compression type

Salt

Key check val

Encrypted and MACed Data

Consider a scenario in which Alice wishes to send important information to Bob using WinZip AE-2 encryption.

Desired functionality

Alice

Bob

Desired functionality

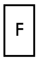
Alice Bob

passphase passphase

Desired functionality

Alice Bob

passphase passphase


F

Desired functionality

Alice Bob

passphase passphase

F WinZip

Desired functionality

Alice Bob

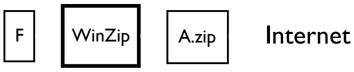
passphase passphase

F WinZip A.zip

Desired functionality

Alice Bob

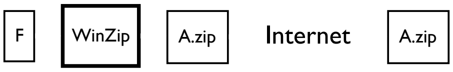
passphase passphase


F WinZip A.zip Internet

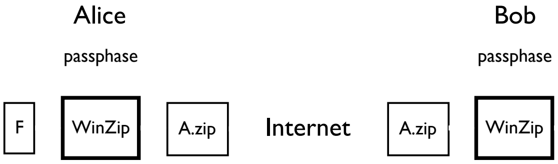
Desired functionality

Alice Bob

passphase passphase


F WinZip A.zip Internet A.zip

Desired functionality


Alice

passphase

Bob

passphase

F

WinZip

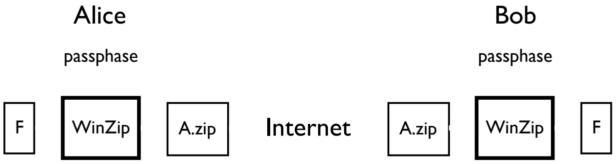
A.zip

Internet

A.zip

WinZip

Desired functionality


Alice

passphase

Bob

passphase

F

WinZip

A.zip

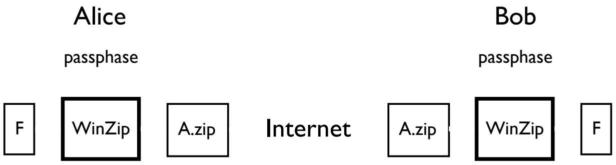
Internet

A.zip

WinZip

F

First security goal (privacy)


Alice

passphase

Bob

passphase

F

WinZip

A.zip

Internet

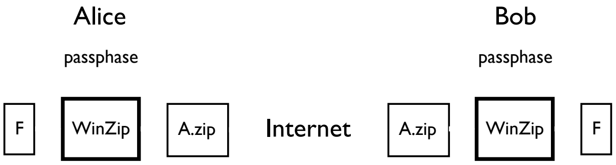
A.zip

WinZip

F

Important!! Different classes of adversaries. Unknown plaintext, known plaintext, chosen plaintext, chosen ciphertext

First security goal (privacy)


Alice

passphase

Bob

passphase

F

WinZip

A.zip

Internet

A.zip

WinZip

F

Even if Mallory is able to learn A.zip, he should not be able to learn useful information about the original file F.

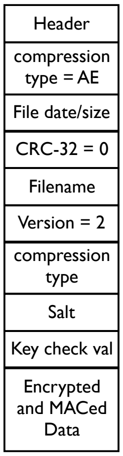
Important!! Different classes of adversaries. Unknown plaintext, known plaintext, chosen plaintext, chosen ciphertext

Information leakage

From A.zip, the adversary can learn

- The names of the encrypted files.
- The files' last modification dates and times.
- The files' compression ratios.

Unknown plaintext, known plaintext, and chosen-plaintext issues


Header

compression type = AE

File date/size

CRC-32 = 0

Filename

Version = 2

compression type

Salt

Key check val

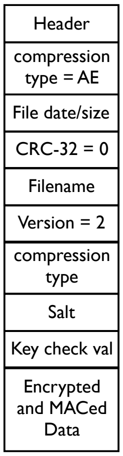
Encrypted and MACed Data

Information leakage

From A.zip, the adversary can learn

- The names of the encrypted files.
- The files' last modification dates and times.
- The files' compression ratios.

Unknown plaintext, known plaintext, and chosen-plaintext issues


Header

compression type = AE

File date/size

CRC-32 = 0

Filename

Version = 2

compression type

Salt

Key check val

Encrypted and MACed Data

Information leakage

Potentially serious. For example,

- Not uncommon for filenames to contain personal or sensitive information.
- Compression ratios of files, and especially of related files, can leak information about those files' contents [BCL02,Kel02].

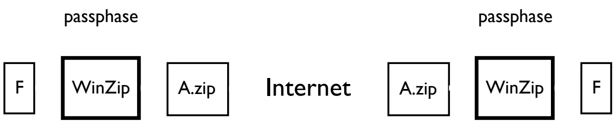
Information leakage

Potentially serious. For example,

- Not uncommon for filenames to contain personal or sensitive information.
- Compression ratios of files, and especially of related files, can leak information about those files' contents [BCL02,Kel02].

Information leakage was a problem with classic WinZip encryption, so the problem should have been fixed with AE-2.

Second security goal (authenticity)



Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

Second security goal (authenticity)

Alice
passphase
Bob
passphase
F
WinZip
A.zip
A.zip
WinZip
F

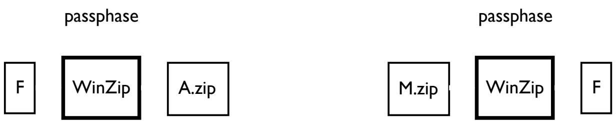
Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

Second security goal (authenticity)

Alice
passphase
Bob
passphase
F
WinZip
A.zip
WinZip
F

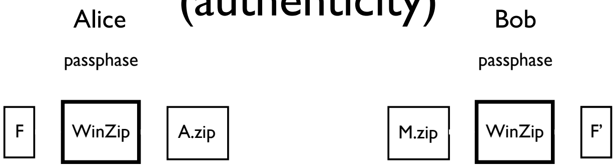
Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

Second security goal (authenticity)



Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

Second security goal (authenticity)


Alice

passphase

F

WinZip

A.zip

M.zip

WinZip

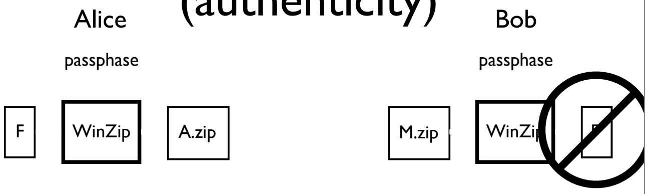
F'

Bob

passphase

Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

Second security goal (authenticity)


Alice

passphase

F

WinZip

A.zip

M.zip

WinZi

F

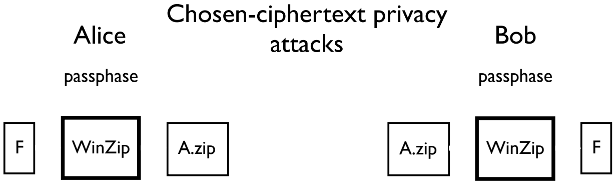
Bob

passphase

Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

Third security goal (privacy)

Chosen-ciphertext privacy attacks


Alice

passphase

F

WinZip

A.zip

A.zip

WinZip

F

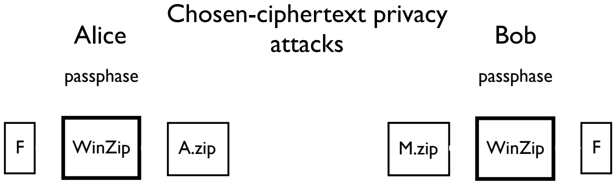
Bob

passphase

Even if Mallory can modify A.zip in transit and can learn Bob's output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

Chosen-ciphertext privacy attacks


Alice

passphase

F

WinZip

A.zip

M.zip

WinZip

F

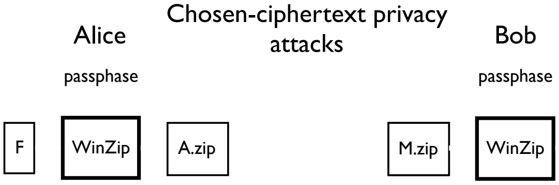
Bob

passphase

Even if Mallory can modify A.zip in transit and can learn Bob's output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

Chosen-ciphertext privacy attacks


Alice

passphase

F

WinZip

A.zip

M.zip

WinZip

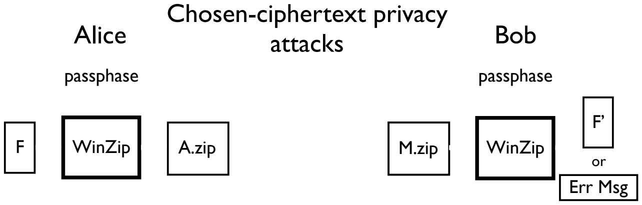
Bob

passphase

Even if Mallory can modify A.zip in transit and can learn Bob's output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

Chosen-ciphertext privacy attacks


Alice

passphase

F

WinZip

A.zip

M.zip

WinZip

F'

or

Err Msg

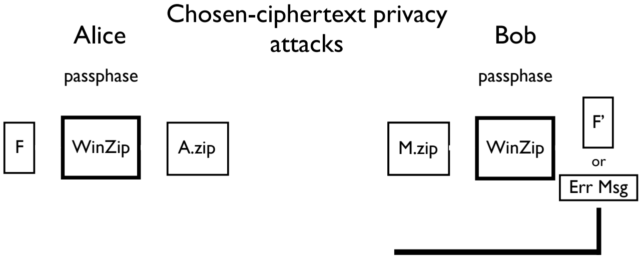
Bob

passphase

Even if Mallory can modify A.zip in transit and can learn Bob's output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

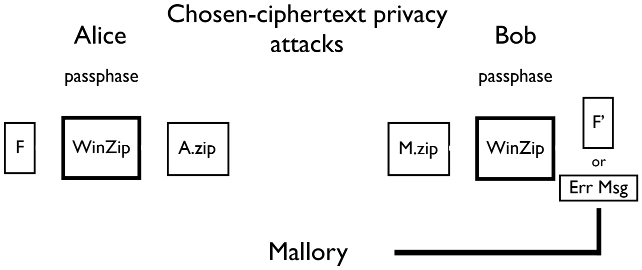
Chosen-ciphertext privacy attacks



Even if Mallory can modify A.zip in transit and can learn Bob’s output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

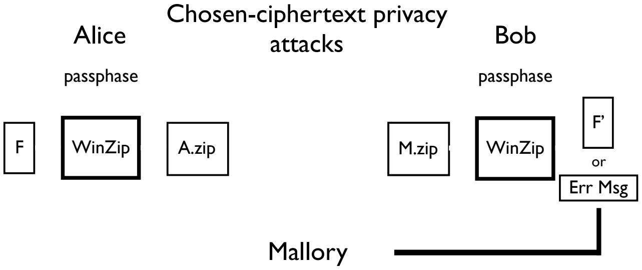
Chosen-ciphertext privacy attacks



Even if Mallory can modify A.zip in transit and can learn Bob’s output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

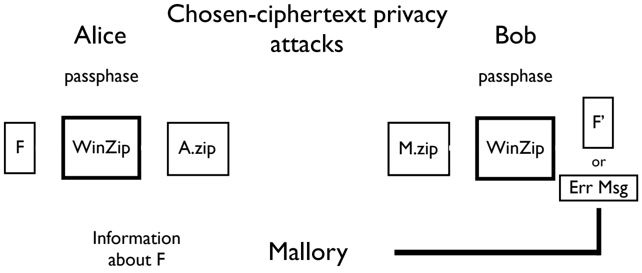
Chosen-ciphertext privacy attacks



Even if Mallory can modify A.zip in transit and can learn Bob’s output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

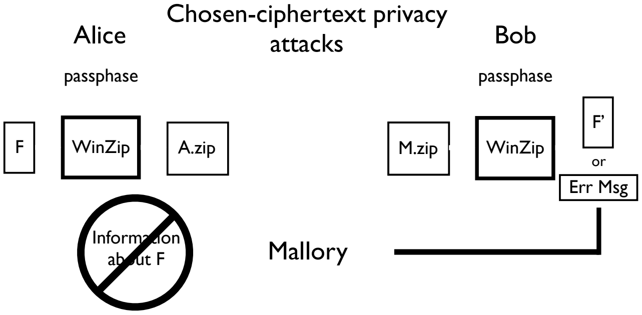
Chosen-ciphertext privacy attacks



Even if Mallory can modify A.zip in transit and can learn Bob’s output, Mallory should not be able to learn additional information about F.

Third security goal (privacy)

Chosen-ciphertext privacy attacks



Even if Mallory can modify A.zip in transit and can learn Bob’s output, Mallory should not be able to learn additional information about F.

A.zip

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

A.zip
Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

The “Encrypted and MACed Data” field of A.zip contains the contents of the file F, only compressed and encrypted.

A.zip	M.zip
Header	Header
compression type = AE	compression type = AE
File date/size	File date/size
CRC-32 = 0	CRC-32 = 0
Filename	Filename
Version = 2	Version = 2
compression type	compression type
Salt	Salt
Key check val	Key check val
Encrypted and MACed Data	Encrypted and MACed Data - prime

The “Encrypted and MACed Data” field of A.zip contains the contents of the file F, only compressed and encrypted.

Therefore, an adversary might try to break the authenticity by creating a new M.zip based on A.zip, but with this field changed.

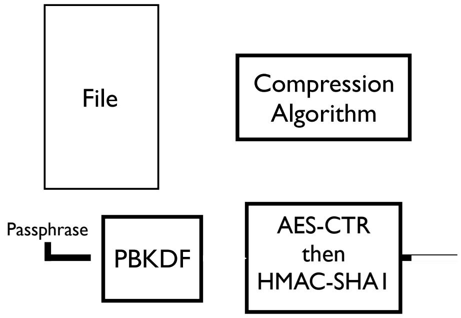
A.zip	M.zip
Header	Header
compression type = AE	compression type = AE
File date/size	File date/size
CRC-32 = 0	CRC-32 = 0
Filename	Filename
Version = 2	Version = 2
compression type	compression type
Salt	Salt
Key check val	Key check val
Encrypted and MACed Data	Encrypted and MACed Data - prime

The “Encrypted and MACed Data” field of A.zip contains the contents of the file F, only compressed and encrypted.

Therefore, an adversary might try to break the authenticity by creating a new M.zip based on A.zip, but with this field changed.

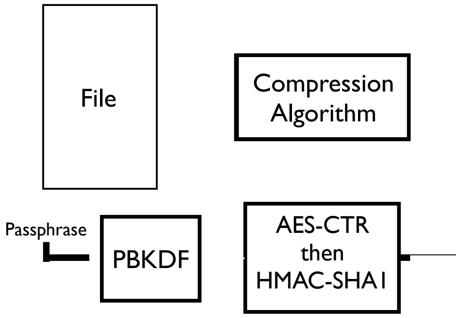
But, because of the MAC, such an attack will generally not work.

Zipping a file with AE-2



Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

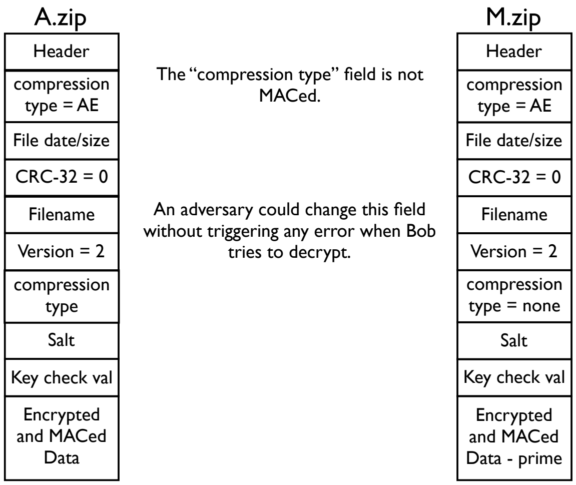
WinZip has the ability to use different compression algorithms. WinZip records the choice in the “compression type” field.



Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

A.zip
Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

The “compression type” field is not MACed.



A.zip

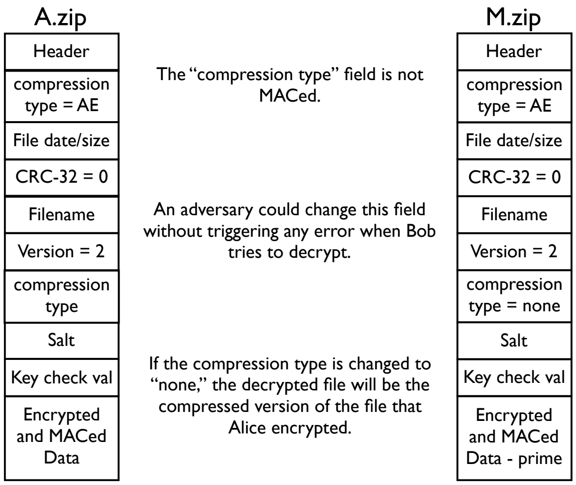
Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

M.zip

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type = none
Salt
Key check val
Encrypted and MACed Data - prime

The "compression type" field is not MACed.

An adversary could change this field without triggering any error when Bob tries to decrypt.



A.zip

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

M.zip

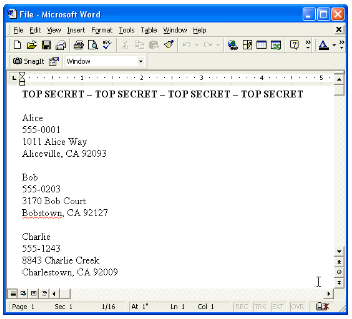
Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type = none
Salt
Key check val
Encrypted and MACed Data - prime

The "compression type" field is not MACed.

An adversary could change this field without triggering any error when Bob tries to decrypt.

If the compression type is changed to "none," the decrypted file will be the compressed version of the file that Alice encrypted.

Illustrating the attack



File - Microsoft Word
File Edit View Insert Format Tools Table Window Help
SnagIt
Window

TOP SECRET – TOP SECRET – TOP SECRET – TOP SECRET

Alice
555-0001
1011 Alice Way
Aliceville, CA 92093

Bob
555-0203
3170 Bob Court
Bobstown, CA 92127

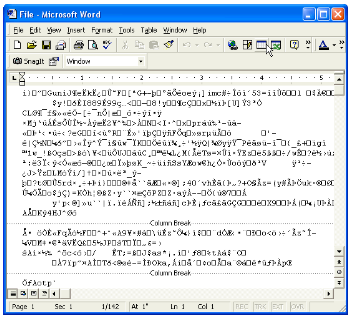
Charlie
555-1243
8843 Charlie Creek
Charlestown, CA 92009

Page 1 Sec 1 1/16 At 1" Ln 1 Col 1 REC TRK EXT OVR

Suppose the file that Alice encrypts looks like this.

Illustrating the attack

If Mallory applies the attack, then the file that Bob extracts will look like this:



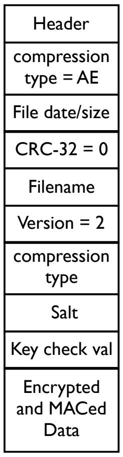
```
í}□″□GuníJ¶eËkË¿□Û˜F□[ªG+-þ□°ãÕêoeý¡] imc#÷Îôì´53=îîÙõ□□1 □$Ä€□□
        $y!□ðÈI889É99ç…<□□—□8!y□□¶cÇ□□x□½ïÞ[U]Ý3³Ò
CLØ¶¯f§»«êÖ-[÷¯nÕ|æ□_ô•÷ýî•ÿ
×Mj`úÁÉsÕÙÎ¼~ÀýæË2¥^‰□>À□N□<I·^□x□práú‰¹-ûà-
«□Þ¹‹ •ú÷‹ ?eG□□î<ù°R□¨É»'ïþÇ□ÿñFÕq□»ørµüÃ□ó       □'-
ê|Ç½N□¼ð″□ ›«Îÿ^Ý¯i§ûw¯ÏK□□Öêûï¾¸÷'½ÿQ|¾ØyÿŸ¯Pêãøü-î¯□(_£+□ïgí
™1w_!ßOçs□>ßó\¥<□üÔUJ□âûC¸□™ê¼L¿M(ÅëTø=¤Ûí×ŸEz□ë5ßß□÷/wÊ□?é½›ú;
ª:ë3Ï‹ ý<Ó«æô—®□□¿œ□Ï»þøK_~÷üiñSsYÆow€h¿Ò×Ùoóý□ð¹V      ÿ¹÷-
¿J>Ÿz□LMóÝí/]†□×□ú×ë³_ý-
þ□?tØ□Û5rd×¸÷+Þi}□□□®‡å``ãÆ□«×®];40´vhÈã(Þ„?+O§Ãz=(y#ÃÞÖuk·®□Ø
Ú¼ÖÃ□o$jÇ)=KÒh¦©ßZ·y``¤æÇõPZ□Z·aýÀ--□Ö(ú®7□□Á
        y'p‹®]»u``|ï.ïèÁÑñ];½±ñáñ]cÞÈ¡ƒcã£ãGÇG□□□è□X9□□ÞÁ(□¼¡UÞÀI
AÅ□Ký4HJ^Øô
..........................Column Break..........................
Å• öÒÈ«FqÃó½F□□^+^«A9¥×#à□\üÉz˜Ô¼)í$□□¨dÒÆ‹ •¨□Ð□o<ö›÷´Ãz˜Î-
¼V□M‡•€ªäVËQ£□5½JP□šT□Ï□„&=›
šAì×½‰ ^õc<ô›□/    ÊT;=ß□J$as*¡.ì□'ƒ8□‰tAá$¨O□
        □À7ïp″¤AÌ□Tð<®øè-=ÌÐOka,Áí□å´□¢o□Å□a¨©á□ê*ûƒÞÀpŒ
..........................Column Break..........................
ÖƒAotp`
```

The previous attack is "conventional:" it focuses on attacking the encryption of the data contained within a file.

The previous attack is "conventional:" it focuses on attacking the encryption of the data contained within a file.

But a file's filename is critical to the interpretation of the data contained within the file.

Attacking filenames



Header

compression type = AE

File date/size

CRC-32 = 0

Filename

Version = 2

compression type

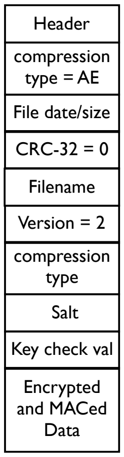
Salt

Key check val

Encrypted and MACed Data

Attacking filenames

The filename field is unauthenticated.



Header

compression type = AE

File date/size

CRC-32 = 0

Filename

Version = 2

compression type

Salt

Key check val

Encrypted and MACed Data

Attacking filenames

Consequences of unauthenticated filenames:

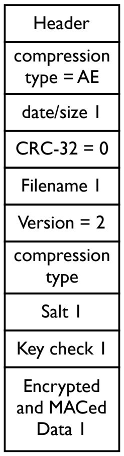
- Break authenticity. E.g., change a file's name from AliceSalary.dat to MallorySalary.dat.
- Break privacy. E.g., change a file's extension from .doc to .xls and observe Bob's response. (Window's default application will be unable to load the file.)

A Zip archive may contain more than one file.

A Zip archive may contain more than one file.

When this is the case, the files' fields are concatenated together.

(Colors indicate fields that vary per file.)



Header

compression type = AE

date/size 1

CRC-32 = 0

Filename 1

Version = 2

compression type

Salt 1

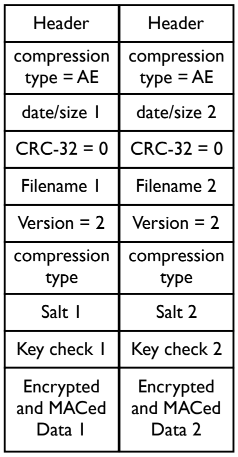
Key check 1

Encrypted and MACed Data 1

A Zip archive may contain more than one file.

When this is the case, the files' fields are concatenated together.

(Colors indicate fields that vary per file.)



Header	Header
compression type = AE	compression type = AE
date/size 1	date/size 2
CRC-32 = 0	CRC-32 = 0
Filename 1	Filename 2
Version = 2	Version = 2
compression type	compression type
Salt 1	Salt 2
Key check 1	Key check 2
Encrypted and MACed Data 1	Encrypted and MACed Data 2

A Zip archive may contain more than one file.

When this is the case, the files' fields are concatenated together.

(Colors indicate fields that vary per file.)

Header	Header	Header
compression type = AE	compression type = AE	compression type = AE
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32 = 0
Filename 1	Filename 2	Filename 3
Version = 2	Version = 2	Version = 2
compression type	compression type	compression type
Salt 1	Salt 2	Salt 3
Key check 1	Key check 2	Key check 3
Encrypted and MACed Data 1	Encrypted and MACed Data 2	Encrypted and MACed Data 3

Since each file is encapsulated separately, not all files need to be encrypted.

Header	Header	Header
compression type = AE	compression type = AE	compression type = AE
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32 = 0
Filename 1	Filename 2	Filename 3
Version = 2	Version = 2	Version = 2
compression type	compression type	compression type
Salt 1	Salt 2	Salt 3
Key check 1	Key check 2	Key check 3
Encrypted and MACed Data 1	Encrypted and MACed Data 2	Encrypted and MACed Data 3

Since each file is encapsulated separately, not all files need to be encrypted.

Header	Header
compression type = AE	compression type = AE
date/size 1	date/size 2
CRC-32 = 0	CRC-32 = 0
Filename 1	Filename 2
Version = 2	Version = 2
compression type	compression type
Salt 1	Salt 2
Key check 1	Key check 2
Encrypted and MACed Data 1	Encrypted and MACed Data 2

Since each file is encapsulated separately, not all files need to be encrypted.

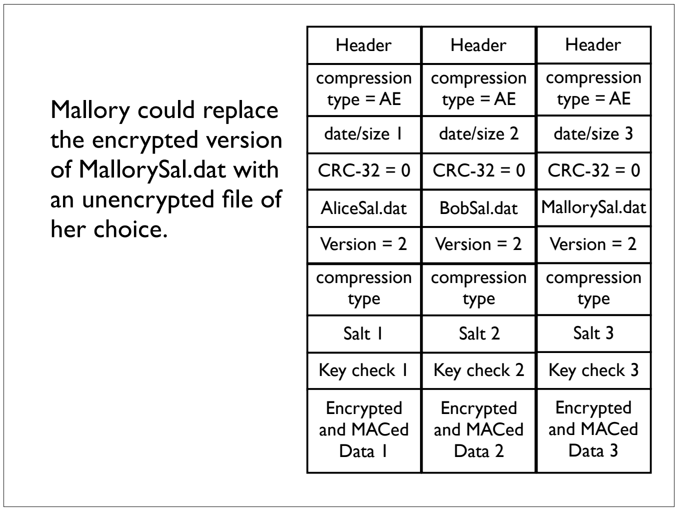
Header	Header	Header
compression type = AE	compression type = AE	compression type
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32
Filename 1	Filename 2	Filename 3
Version = 2	Version = 2	Compressed Data 3
compression type	compression type	
Salt 1	Salt 2	
Key check 1	Key check 2	
Encrypted and MACed Data 1	Encrypted and MACed Data 2	

Suppose a WinZip archive contains Alice's, Bob's, and Mallory's salary.

Header	Header	Header
compression type = AE	compression type = AE	compression type = AE
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32 = 0
AliceSal.dat	BobSal.dat	MallorySal.dat
Version = 2	Version = 2	Version = 2
compression type	compression type	compression type
Salt 1	Salt 2	Salt 3
Key check 1	Key check 2	Key check 3
Encrypted and MACed Data 1	Encrypted and MACed Data 2	Encrypted and MACed Data 3

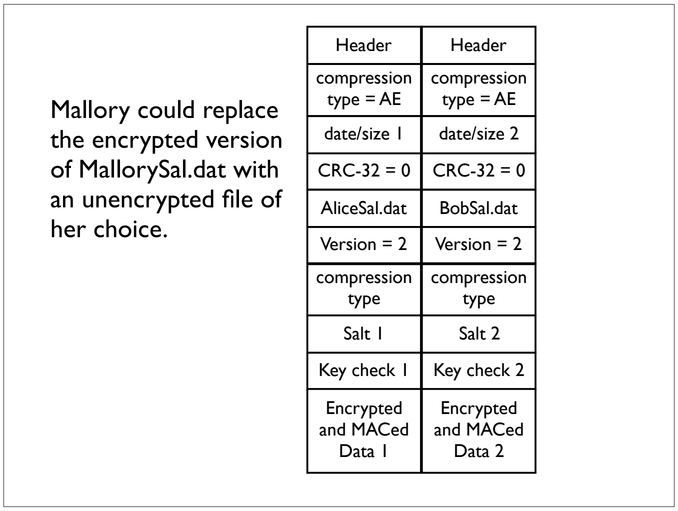
Suppose a WinZip archive contains Alice's, Bob's, and Mallory's salary.

Header	Header	Header
compression type = AE	compression type = AE	compression type = AE
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32 = 0
AliceSal.dat	BobSal.dat	MallorySal.dat
Version = 2	Version = 2	Version = 2
compression type	compression type	compression type
Salt 1	Salt 2	Salt 3
Key check 1	Key check 2	Key check 3
Encrypted and MACed Data 1	Encrypted and MACed Data 2	Encrypted and MACed Data 3



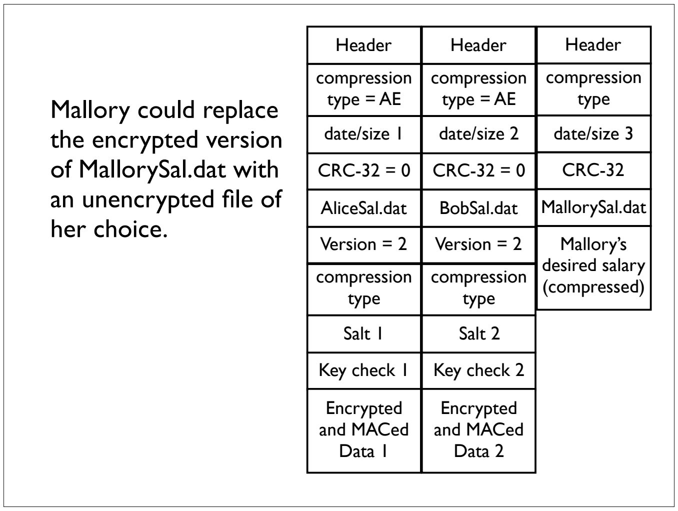
Mallory could replace the encrypted version of MallorySal.dat with an unencrypted file of her choice.

Header	Header	Header
compression type = AE	compression type = AE	compression type = AE
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32 = 0
AliceSal.dat	BobSal.dat	MallorySal.dat
Version = 2	Version = 2	Version = 2
compression type	compression type	compression type
Salt 1	Salt 2	Salt 3
Key check 1	Key check 2	Key check 3
Encrypted and MACed Data 1	Encrypted and MACed Data 2	Encrypted and MACed Data 3



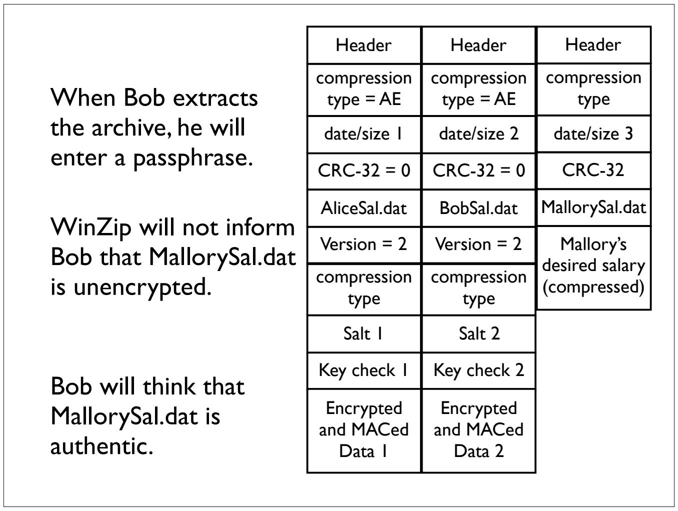
Mallory could replace the encrypted version of MallorySal.dat with an unencrypted file of her choice.

Header	Header
compression type = AE	compression type = AE
date/size 1	date/size 2
CRC-32 = 0	CRC-32 = 0
AliceSal.dat	BobSal.dat
Version = 2	Version = 2
compression type	compression type
Salt 1	Salt 2
Key check 1	Key check 2
Encrypted and MACed Data 1	Encrypted and MACed Data 2



Mallory could replace the encrypted version of MallorySal.dat with an unencrypted file of her choice.

Header	Header	Header
compression type = AE	compression type = AE	compression type
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32
AliceSal.dat	BobSal.dat	MallorySal.dat
Version = 2	Version = 2	Mallory's desired salary (compressed)
compression type	compression type	
Salt 1	Salt 2	
Key check 1	Key check 2	
Encrypted and MACed Data 1	Encrypted and MACed Data 2	

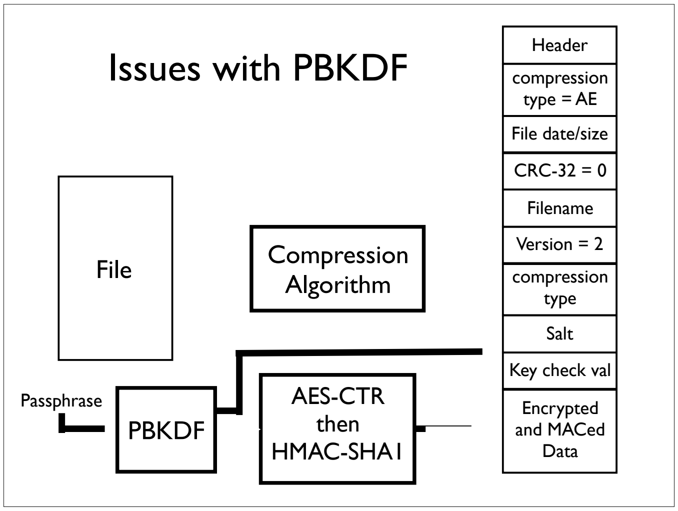


When Bob extracts the archive, he will enter a passphrase.

WinZip will not inform Bob that MallorySal.dat is unencrypted.

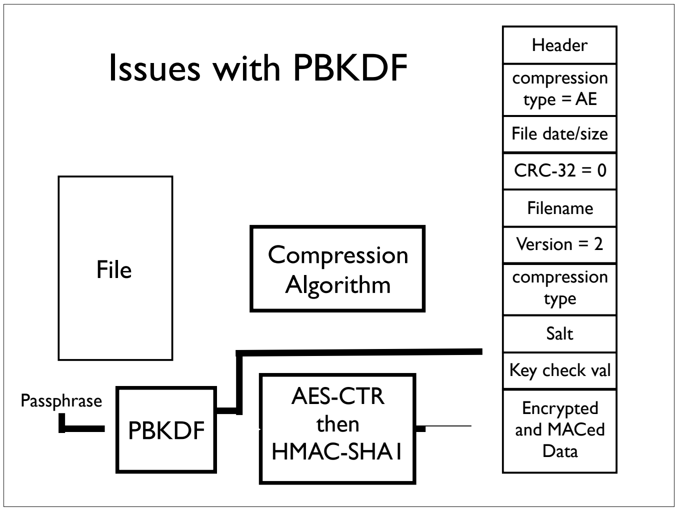
Bob will think that MallorySal.dat is authentic.

Header	Header	Header
compression type = AE	compression type = AE	compression type
date/size 1	date/size 2	date/size 3
CRC-32 = 0	CRC-32 = 0	CRC-32
AliceSal.dat	BobSal.dat	MallorySal.dat
Version = 2	Version = 2	Mallory's desired salary (compressed)
compression type	compression type	
Salt 1	Salt 2	
Key check 1	Key check 2	
Encrypted and MACed Data 1	Encrypted and MACed Data 2	



Issues with PBKDF

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data



Issues with PBKDF

Header
compression type = AE
File date/size
CRC-32 = 0
Filename
Version = 2
compression type
Salt
Key check val
Encrypted and MACed Data

PBKDF

The PBKDF module derives AES and HMAC-SHA1 keys from a user's passphrase and a randomly selected salt.

PBKDF is parameterized.

When deriving 128-bit AES keys, WinZip will use a 64-bit salt.

AES key collisions

If the user encrypts 2^{32} files with the same passphrase, then we expect two files to use the same 64-bit salt.

The AES key is a deterministic function of the passphrase and the salt.

Therefore, we expect AES key collisions after encrypting only 2^{32} files.

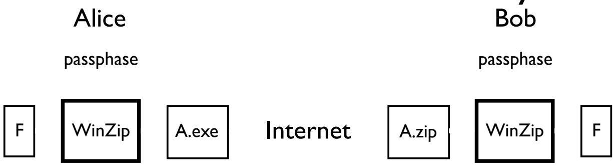
Keystream reuse

WinZip always uses AES-CTR with zero as the initial counter.

An AES key collision implies keystream reuse.

Therefore, we expect AES-CTR keystream reuse after encrypting only 2^{32} files.

Self-extracting Encrypted Executables and Authenticity


Alice

Bob

passphase

passphase

F

WinZip

A.exe

Internet

A.zip

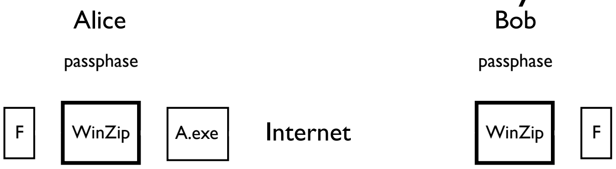
WinZip

F

Goal: Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

But M.exe is an executable! Replace M.exe with a malicious binary that ignores the passphrase and outputs the file F' of the adversary's choice.

Self-extracting Encrypted Executables and Authenticity


Alice

Bob

passphase

passphase

F

WinZip

A.exe

Internet

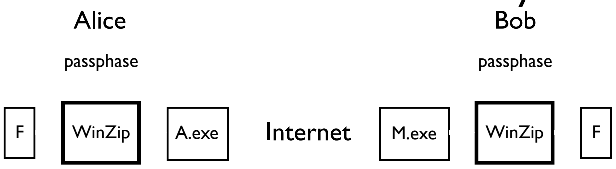
WinZip

F

Goal: Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

But M.exe is an executable! Replace M.exe with a malicious binary that ignores the passphrase and outputs the file F' of the adversary's choice.

Self-extracting Encrypted Executables and Authenticity


Alice

Bob

passphase

passphase

F

WinZip

A.exe

Internet

M.exe

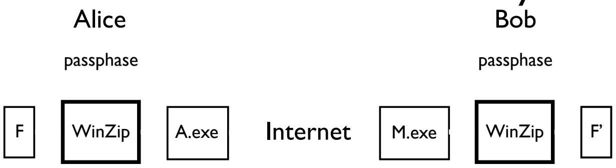
WinZip

F

Goal: Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

But M.exe is an executable! Replace M.exe with a malicious binary that ignores the passphrase and outputs the file F' of the adversary's choice.

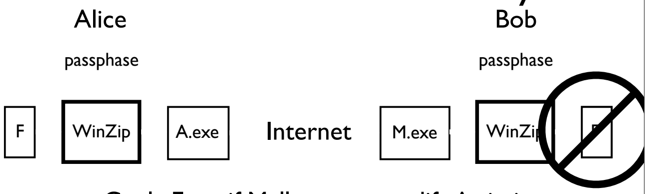
Self-extracting Encrypted Executables and Authenticity



Goal: Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

But M.exe is an executable! Replace M.exe with a malicious binary that ignores the passphrase and outputs the file F' of the adversary's choice.

Self-extracting Encrypted Executables and Authenticity



Goal: Even if Mallory can modify A.zip in transit, he should not be able to trick Bob into accepting a file that Alice did not send.

But M.exe is an executable! Replace M.exe with a malicious binary that ignores the passphrase and outputs the file F' of the adversary's choice.

Now to the Whiteboard

- Attacking
  - CTR mode encryption with 0 as the IV
    - State assumptions
    - Make assumptions about what adversary knows
    - Show that the adversary can learn new things under some model (unknown plaintext, known plaintext, chosen plaintext)
  - CBC mode where the IV for the i-th message is the last ciphertext block of the (i-1)-st message
    - chosen-plaintext attack
  - Creating a MAC from with a hash function H as Tag (K,M) = H(K||M), where || denotes string concatenation