The Story of Alice and her Boss:

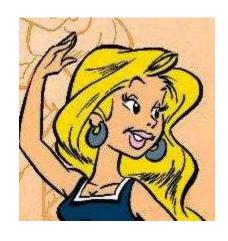
Hash Functions and the Blind Passenger Attack

Stefan Lucks $^{\cal M}$, Magnus Daum $^{\cal B}$

 M University of Mannheim, Germany B Ruhr-University Bochum, Germany

Alice and her Boss (1)

 Caesar writes letter of recommendation.



2. Email from Alice: "please digitally sign the attached letter".



3. Caesar views file. OK! Email from Caesar: signature.

Alice and her Boss (2)

Alice: different document, forge Caesar's signature.

But:

- target fixed (Caesar's letter).
- Alice only knows how to generate "random" collision.
- The end of the story?

MD5 "Target Collisions"

given target

colliding order

... fulfilled all the requirements ... I highly recommend hiring her.

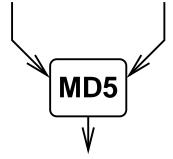
Sincerely,

Julius Caesar

... full access to all confidential and secret information ...

Sincerely,

Julius Caesar



5421a523481fdc6a2a1c832e72c7b8a5

Helping Alice (1)

- 1. Use "advanced" document language (PostScript).
- 2. Find random strings R_1 and R_2 and concatenate to some preamble:

$$X_1 = \mathsf{preamble}; \; \mathsf{put}(R_1);$$

$$X_2 = \mathsf{preamble}; \; \mathsf{put}(R_2);$$

$$MD5(X_1)=MD5(X_2).$$

Eurocrypt 2005!

Appending a string S to both X_1 and X_2 : MD5($X_1||S$)=MD5($X_2||S$). Well-known weakness!

Helping Alice (2)

The target documents are T_1 and T_2 :

$$Y_1 = \overbrace{\mathsf{preamble};\,\mathsf{put}(R_1);\,\,\mathsf{put}(R_1);\,\,\mathsf{if}(=)\,\,\mathsf{then}\,\,T_1\,\,\mathsf{else}\,\,T_2;}^{X_1}$$
 $Y_2 = \underbrace{\mathsf{preamble};\,\mathsf{put}(R_2);\,\,\,\mathsf{put}(R_1);\,\,\mathsf{if}(=)\,\,\,\mathsf{then}\,\,T_1\,\,\mathsf{else}\,\,T_2;}_{X_2}$

- Viewing Y_1 : $R_1 = R_1$, thus T_1 is displayed.
- Viewing Y_2 : $R_2 \neq R_1$, thus T_2 is displayed.

Remarks

- 1. Techniques to find "random hash collisions" can be used for practical attacks!
- 2. Don't use broken hash functions!
- 3. What about other document languages (Office, ...)?

