Enhancing Security Using Honeywords

Project Group Id: 28
Under guidance of
Mrs. Shital A. Patil.

SSBT'S COET,Bambhori,Jalgaon

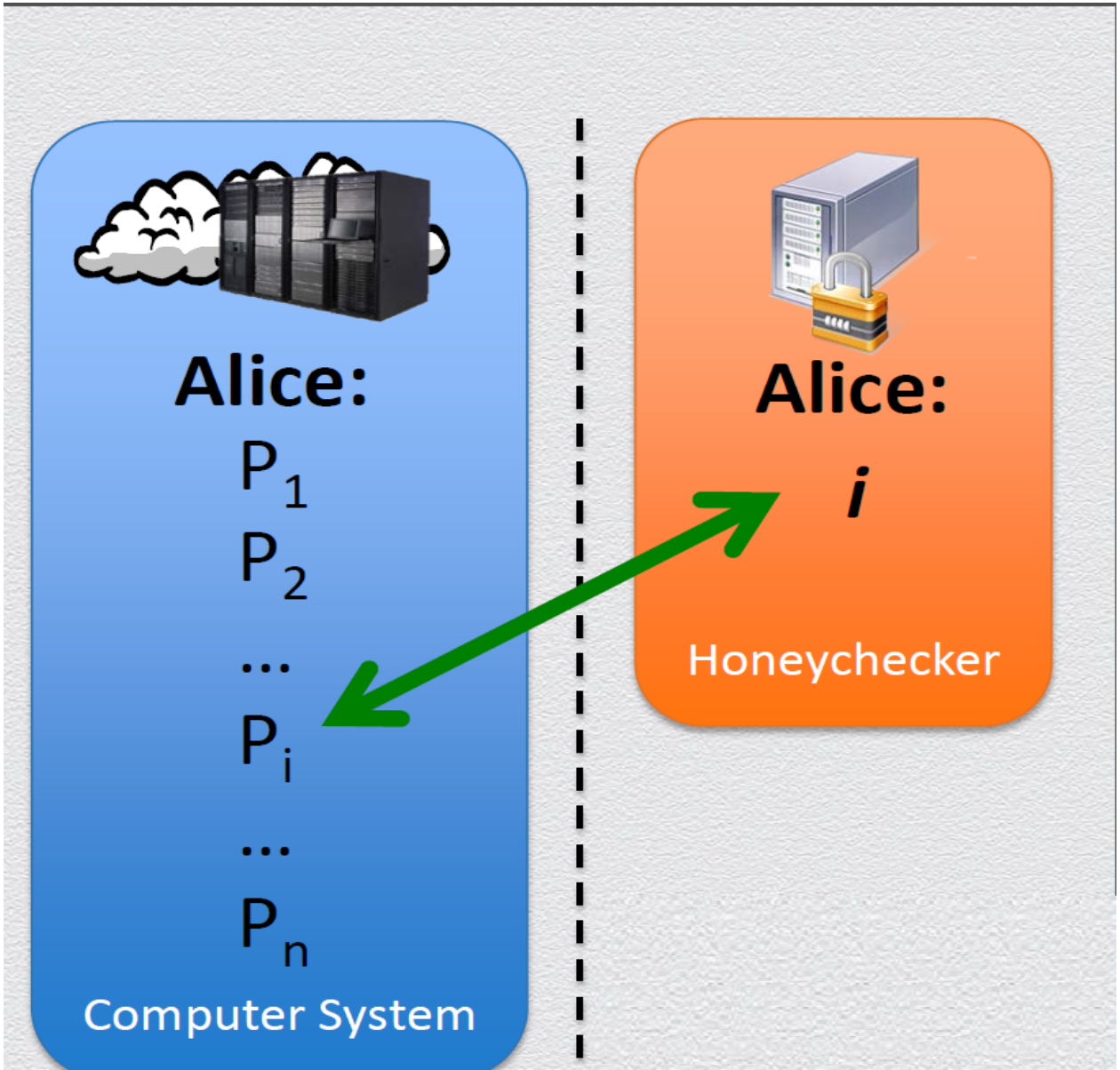
September 27, 2016

Outline

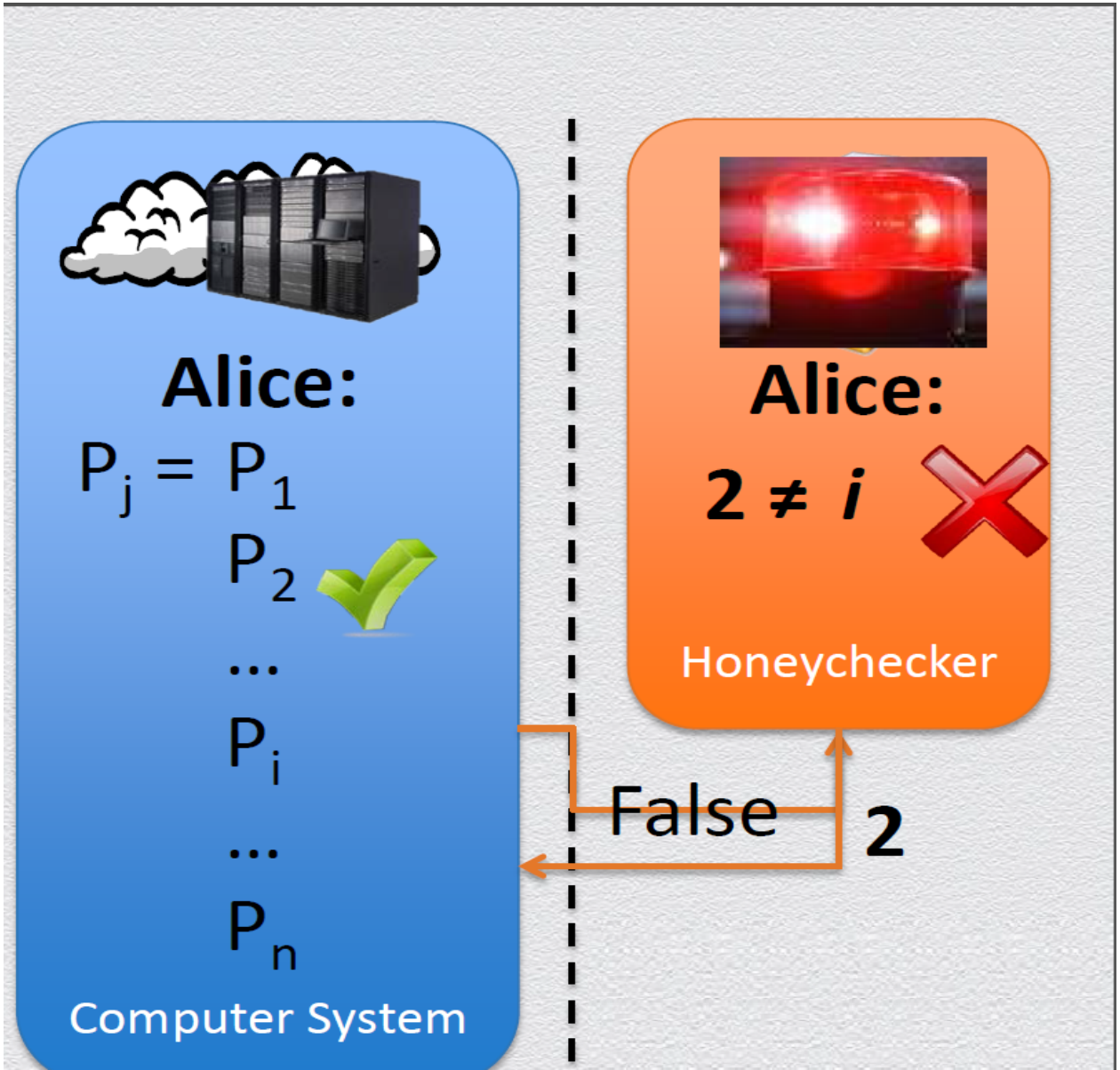
Introduction

- **Motivation** theft of password hash files.
- **Honeywords** enables detection of theft, prevents impersonation.
- Honeywords are **decoy passwords**.

System Overview



System Overview..



Honeywords

- Create additional honeyword passwords.
- Store the honeywords with the real passwords in a hash file
- Incorporate an auxiliary secure server called a honeychecker.
- When a login is attempted, the main server verifies the request with the honeychecker.

Honeyword Generation

- Two types of approaches are used to generate Honeywords.
  1. Chaffing by Tweaking:
  2. Take-a-Tail:

Chaffing by Tweaking

- Tweak selected character positions of the password to obtain the honeywords
- For each selected position the character of the real password is replaced by a randomly-chosen character of the same type
- Alternatives
  1. Chaffing-by-tail-tweaking: tweak last t positions of password
  2. Chaffing-by-tweaking-digits: tweak last t positions containing digits
- Example where t = 5
  Password77 = Pass**H**ord**12** Pass**C**ord**45** Pass**V**ord**67**

take-a-tail

- Request password from user and then modify it with a randomized tail.
- Actual password : Password77
- Generated honeywords :
  Password12
  Password34
  Password56
  Password67
  Password78
  Password90

Hybrid Generation Methods

- Combining several methods can result in better honeywords
- Combine both techniques:
- Require the user to use digits at the end of the password
  1. Chaffing-with-a-password to generate new random words
  2. Chaffing-by-tweaking-digits on all words
- Example:Actual Password:Alice77
  Generated honeywords:
  Alice85 Bob49
  Alice65 Bob14

Case Alteration Method

- Takes full advantage of the case sensitive nature of password authentication systems.
- Uppercase-Lowercase,Lowercase-Uppercase
- Example:
  password
  PASSWORD
  PassWORD
  paSSWORD
  PaSsWoRd
  pAsSwOrD
  PASSword,etc.
- for 8 digit password 256 honeywords can be generated by using this simple approach.

Case Alteration Method...

- If password contain the digits and sysmbols then respective substitution are performed.
- E.g. 1l,2z,3E,4A, 5S,6G, 7T,8g, 9q,0O.
- E.g. !i,@ a,# H,$ s.
- semantic significance can be preserved by using this approach.
- Examples:
  Actual password: p@$$word2459
  passwordzASq
  P@SSWORDz4S9
  Pa$$WORD2A5q
  p@S $WORDzA59
  PaS$WoRd2459
  p@sSwOrD2AS9
  PA$Sword24Sq,etc.

Advantages

- simple algorithm.
- No additional database is required for chaffing.
- Overhead of additional stuffing is absent.
- generated honeywords looks similar in appearance making it difficult to guess.
- for recommended storage of 20 honeywords per user 95% security is assured.
- In worst case scenario also 50% security is assured.

Disadvantages

- Recommended set of 20 honeywords per user for obtaining 95% security increases size of password hash files significantly.
- distributed security system is required.
- implementation of additional server called honeychecker is required.

conclusion

- Eventually, passwords should be supplemented with stronger and more convenient authentication methods.
- A simple and powerful new line of defence in the security of hashed passwords.
- Decreases the value of the stolen password hash files.
- Makes password cracking detectable.