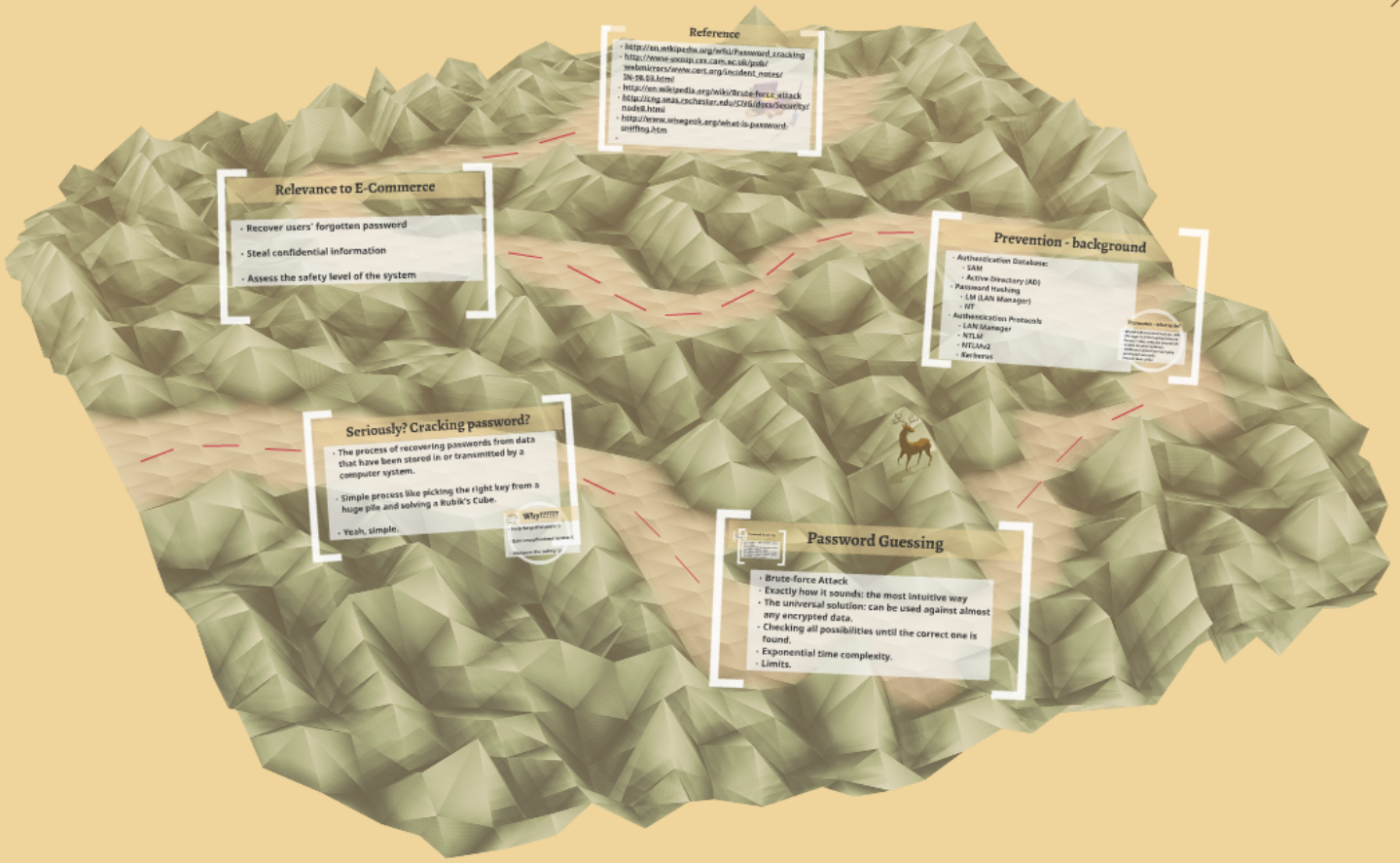
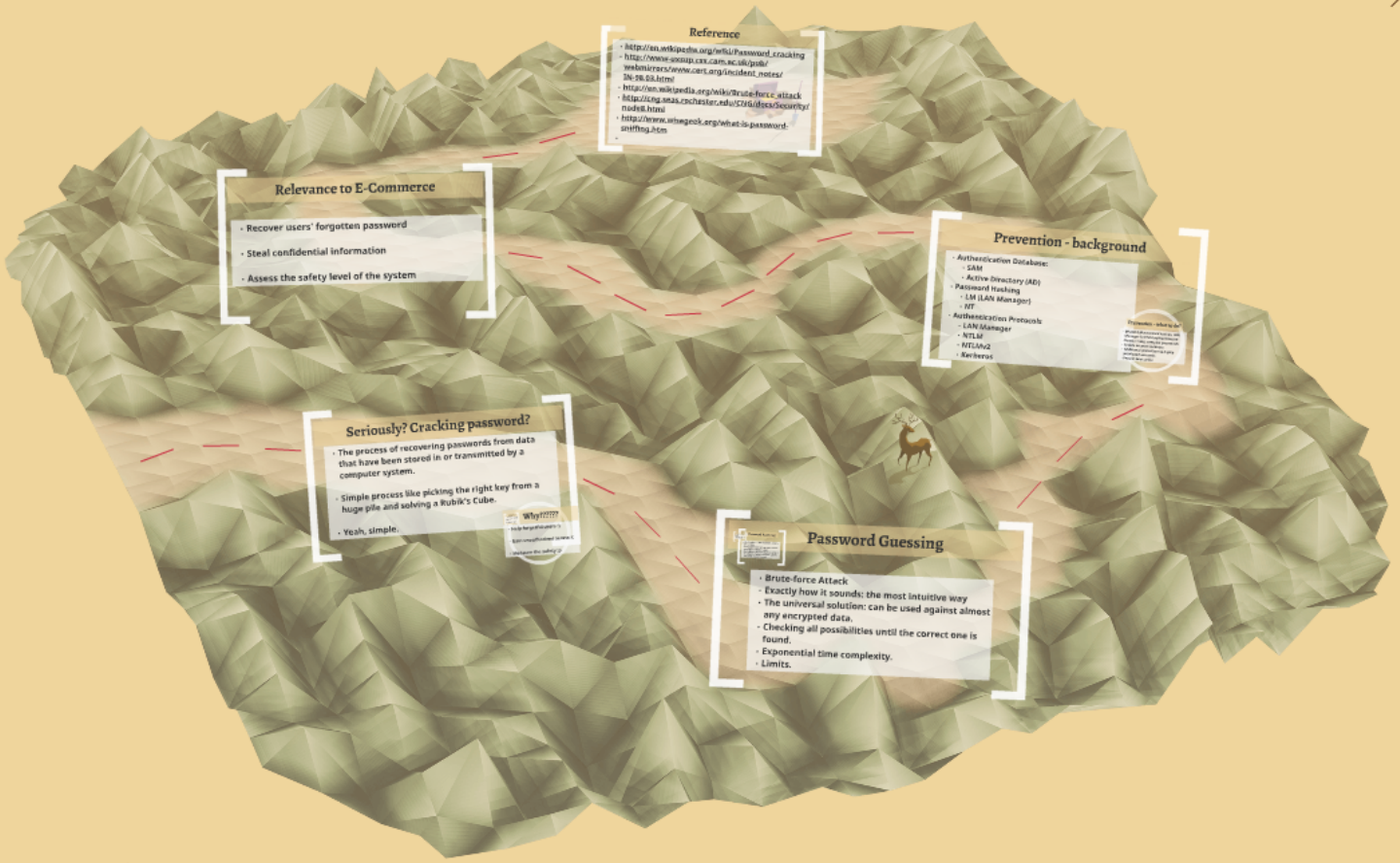
Password Cracking



Password Cracking



Seriously? Cracking password?

- The process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Simple process like picking the right key from a huge pile and solving a Rubik's Cube.
- Yeah, simple.

Why??????

- Help forgetful users :)
- Gain unauthorized access :(
- Measure the safety :p

Incidents?

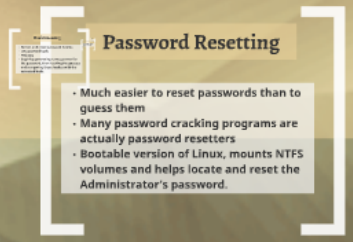
- Attack reported by CERT, July 1998
- Password breach of rockyou.com, Dec 2009
- Ban of password "123456" by Microsoft Hotmail, July 2011

Why??????

- Help forgetful users :)
- Gain unauthorized access :(
- Measure the safety :p

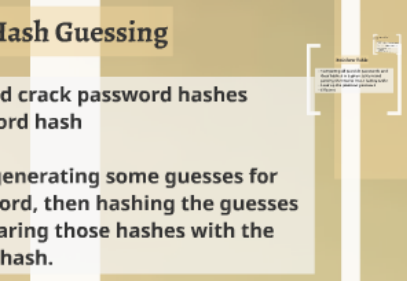
Incidents?

- Attack reported by CERT, July 1998
- Password breach of rockyou.com, Dec 2009
- Ban of password "123456" by Microsoft Hotmail, July 2011



Password Guessing

- Brute-force Attack
- Exactly how it sounds: the most intuitive way
- The universal solution: can be used against almost any encrypted data.
- Checking all possibilities until the correct one is found.
- Exponential time complexity.
- Limits.

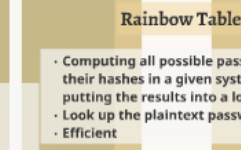


Password Resetting

- Much easier to reset passwords than to guess them
- Many password cracking programs are actually password resetters
- Bootable version of Linux, mounts NTFS volumes and helps locate and reset the Administrator's password.

Hash Guessing

- Extract and crack password hashes
- LM password hash
- Pwdump
- Begin by generating some guesses for the password, then hashing the guesses and comparing those hashes with the extracted hash.



- Examining individual packets of data
- Some password sniffers:
  - SniffPass
  - Password Sniffer Spy

Rainbow Table

- Computing all possible passwords and their hashes in a given system and putting the results into a lookup table
- Look up the plaintext password
- Efficient

Password Sniffing

- Following the traffic across the network
- Examining individual packets of data
- Some password sniffers:
  - SniffPass
  - Password Sniffer Spy

Prevention - background

- Authentication Database:
  - SAM
  - Active Directory (AD)
- Password Hashing
  - LM (LAN Manager)
  - NT
- Authentication Protocols
  - LAN Manager
  - NTLM
  - NTLMv2
  - Kerberos

Prevention - what to do?

- Disable LM password hashes, LAN Manager & NTLM authentication
- Require long, complex passwords
- Enable account lockouts
- Additional protection to highly privileged accounts
- Protect boot order

Prevention - what to do?

- Disable LM password hashes, LAN Manager & NTLM authentication
- Require long, complex passwords
- Enable account lockouts
- Additional protection to highly privileged accounts
- Protect boot order

Relevance to E-Commerce

- Recover users' forgotten password
- Steal confidential information
- Assess the safety level of the system

Reference

- http://en.wikipedia.org/wiki/Password_cracking
- http://www-uxsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/incident_notes/IN-98.03.html
- http://en.wikipedia.org/wiki/Brute-force_attack
- http://cng.seas.rochester.edu/CNG/docs/Security/node8.html
- http://www.wisegeek.org/what-is-password-sniffing.htm

Password Cracking