

# Secure Passwords without Tears: Using Pass Phrases



**To: IT Governance Executive Committee**  
**From: IT Governance Standards & Support Committee**

**Denny Mosier, Chair (I&IT)**  
**Dr. Zekeriya Aliyazicioglu, Engineering**  
**Al Arboleda, I&IT**  
**Ken Bonner, University Advancement**  
**Eric Emerson, SAITS**  
**Alain Gyger (Resource), University Police**  
**Chris Laasch, SAITS**  
**Tim Lockhart, Administrative Affairs**  
**Dr. Shahnaz Lotfipour, CEIS**  
**Ernesto Rodriguez, Academic Affairs**  
**Jane Self, Administrative Affairs**  
**Dr. Mandayam Srinivas, Associate Dean, College of Science**

# Agenda

- How Secure Is Your Password?
- The Current Situation
- How Can the Situation Affect You?
- The Solution
- Recommended Guidelines
- What We Are asking
- Implementation / Timelines
- How Passwords can be Cracked
- Feedback

# Password Breaking Demo

**Host: Chris Laasch**

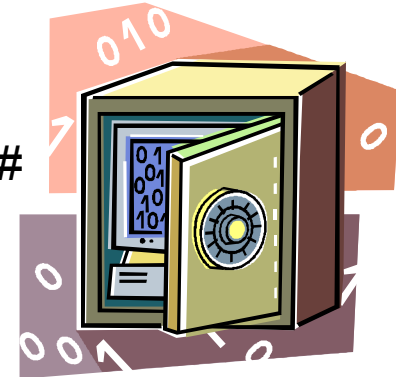
**Hacker: Alain Gyger**

We need two volunteers to create a 14 character complex password using the current CPP complexity standards.

Include three of the following four options:

- Uppercase letter(s)
- Lowercase letter(s)
- Special character(s) i.e.. \$\*!@#
- Number(s)

*For example: ?^%\$D98^%~ah^r*



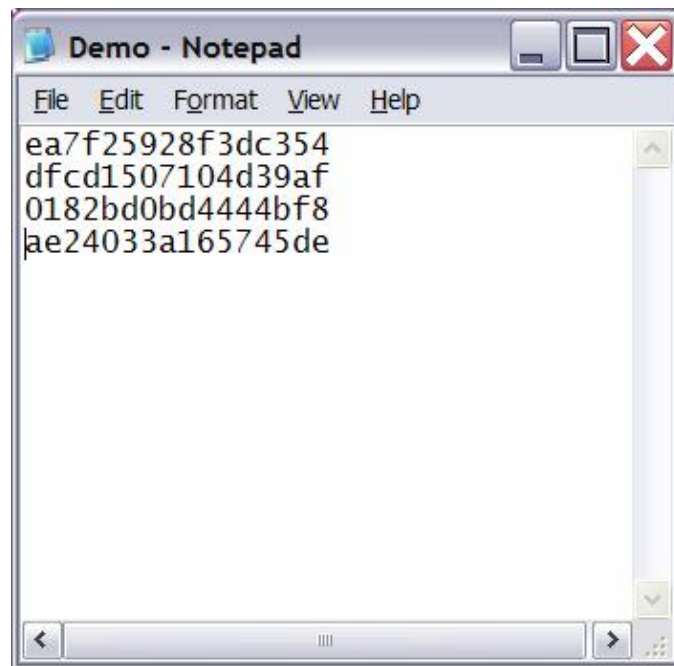
# Two Questions:



1. Which is harder to break, a password like: "I can remember this." or a 14 character password like "@#F{t67M\*9ioE2\$%"
2. How long will it take to break a 14 character password?

# How We Are Breaking Your Passwords

1. Take your passwords, encrypt them with the same algorithm used by Windows.
2. Save them in a file and give it to Alain to decrypt.



# The Current Situation

Al Arboleda

How would your behavior change if your wallets, homes and mail boxes could be accessed from around the world like our computers can?



# Universal Access...

- There are an estimated 304 million people with Internet access
- All 304 million of them can communicate with your CPP connected computer
- Any of the 304 million can rattle the door to your computer to see if it's locked

# Opportunities for Abuse...

- To break into a safe, the safe cracker needs to know something about safes.
- To break into a computer, the computer Hacker only needs to know where to download a program written by someone else who knows something about computers.
- Such programs are freely available all over the net.
- To break into a computer at **CPP**, the hacker need only determine the password; ***our user names are already public***



# How Can the Situation Affect You?...

- A compromised computer provides access to all accounts, keystrokes, and data. Account and keystroke information can be used to access other resources
  - Protected information (e.g., SSNs, Drivers' License #s, Credit Cards, students records)
  - Email and documents
  - Financial transactions
  - Identity theft
  - Criminal use of computer

# Stolen, Hacked Computers

- UCLA: hacker exposed 800,000 current, former students' names, private data
- Berkeley: hacker nabbed 98,000 names, SSNs
- Veterans Affairs: laptop stolen containing 26.5 million personal veteran records
- Croucher: New Zealand brewer offering life-time supply of beer for whoever returns stolen laptop



# The Problem Here

- Until FISMA, KPMG Audits, no secure password guidelines, directives or standards
- Thousands of CPP computers (and some servers) have simple, easy-to-crack passwords that have not been changed in years
- We have been hacked previously many times, primarily because of simple passwords
  - 7 **identified** instances so far this calendar year
  - We have sent two letters to victims of breaches
  - Remember 2005? 1 breach, 32,000 notifications costing us \$200,000 to respond
- Faculty computers are now mobile

# Available Options...

Dr. Mandayam Srinivas

- **Eliminate access**

- If bad guys cannot get to the computer, they cannot break in
- Networks were created to communicate
- Freedom to communicate is key in an academic setting

- **Adopt Pass Phrases**

- Indiana University
- Notre Dame
- University of Minnesota
- Yale
- San Diego State
- Chico State
- Cal Poly Pomona Next??



# Solution:

## A Four-Word Pass Phrase

- **A Sentence**
  - I like ice cream.
  - Turn Off Cell Phones!
  - It was hot today.
  - Cal Poly Broncos rule!



# Audits & Others

- Audits address the BroncoPassword ONLY
- There are thousands of computers with different passwords
- Our recommendations will go hand-in-hand with Audit Findings, ISO's Recommendations

# Change Your Pass Phrase

- Every 120 days
- Students, Faculty, Staff
- We have Challenge Questions installed to Verify identity



# Recommended Guidelines

- A 4-word Pass Phrase for desktops, laptops that follow ISO complex password guidelines
- ISO guidelines – 3 of the 4:
  - At Least One Upper case letter
  - At Least One Lower case letter
  - At Least One Number
  - At Least One Special Character ( # & ! % [space] )
- Phase in over time

# What We are Asking

- IT Governance Executive Committee Endorse Our Recommended Guidelines as support to ISO's recommendations
- Time for each division to Use Guidelines to Improve Computer Security
  - Education
  - Verifying Usage

# Implementation Process

- Who is on board so far:
  - **Academic Senate Tech Committee** Approval = Complete\*
  - **Campus Tech\_Group** Approval = Complete
  - **Academic Affairs Techs'** Approval = In Progress
  - **Advancement Techs'** Approval = Complete
  - **Administrative Affairs Techs'** Approval = In Progress
  - **Student Affairs** Approval = In Progress
  - **ISO** Approval = Complete
  - **I&IT Leadership** Approval = Complete
    - *2006-2007 committee*
- These groups need Guidelines to implement

# Implementation Time Line

- **Communicate To Campus IT Units, End-Users = January 2008 - May 2008**
- **Campus IT Units Roll Out Practice (verification of usage) = Beginning March, 2008**

# How We Did it..

Chris Laasch

## Windows Password Overview

- Windows stores your username and password in a file called “SAM”
- Passwords in this file are encrypted with a flawed technique that is inherently weak. (Blame IBM, not Microsoft for this one!)
- Microsoft's solution: “The simplest way to prevent Windows from storing an LM hash of your password is to use a password that is at least 15 characters long” –MS knowledge base article 299656

# How your password is stored: examples

## Blank or no password

The encryption: AAD3B435B51404EE

7 character password

AAD3B435B51404EE

7 character password

## 7 Character Password

The password: 6D4Nuf\$

The encryption: B6926C56AB6A2E1F

7 character password

AAD3B435B51404EE

7 character password

## 14 Character Password

The password: hg#X468^\_P{sf3

The encryption: 40B9AA7872DF1F71

7 character password

CB65C7D2375CD89F

7 character password

***This is the reason that technicians have instructed users to use 8 or more characters to create a password.***

# Encryptions, Lookups

Since we can easily determine the encrypted values, couldn't we just look up the password like we would look up a word in the dictionary?

## Sample Lookup Table

<u>Password</u>	<u>Encrypted value</u>	<u>Time to break</u>
A	7584248b8d2c9f9e aad3b435b51404ee	< 5 seconds
B	902139606b6d16b5 aad3b435b51404ee	< 5 seconds
C	f9393d97e7a1873c aad3b435b51404ee	< 5 seconds
...		
ZZZZZZZZZZZZZZZZZZZZ	cbc501a4d2227783 cbc501a4d2227783	4.5 minutes

# Conclusion

**A pass phrase composed with four words and punctuation is stronger than all 14 character complex passwords.**

***Our previous sample pass phrase:***

“I can remember this.”

Contains 3 of the 4 ISO requirements to comply with the FISMA, KPMG Audits.

Is greater than 15 characters, so it is not saved into the SAM file as two 7 character passwords. Lookup tables are useless!

***Our previous complex password “@#F{t67M\*9ioE2\$%”***

Contains Upper case letters, Lower case letters, Numbers, and Special characters.

We broke this password in ? minutes using a simple laptop, just like the ones that most students on this campus use everyday.

# Feedback

- IT Governance Executive Committee



# Please...



# Or...



***...Pending Approval from  
other IT areas listed***