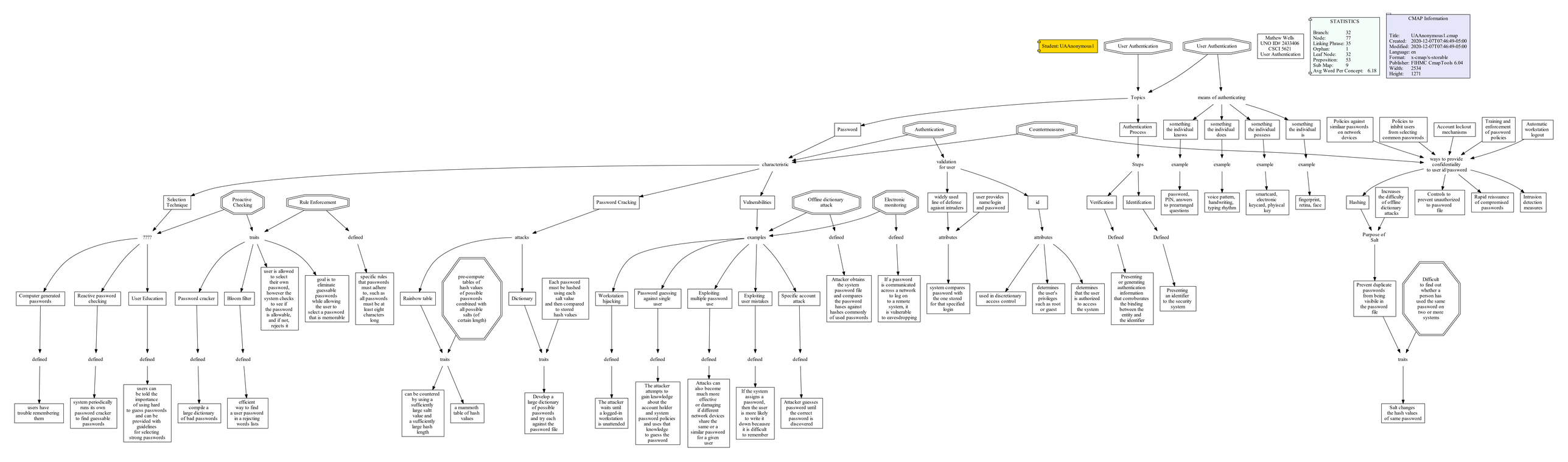
Student: UAAnonymous1
User Authentication
User Authentication
Mathew Wells
UNO ID# 2433406
CSCI 5621
User Authentication
STATISTICS
Branch: 32
Node: 77
Linking Phrase: 35
Orphan: 1
Leaf Node: 32
Preposition: 53
Sub Map: 9
Avg Word Per Concept: 6.18
CMAP Information
Title: UAAnonymous1.cmap
Created: 2020-12-07T07:46:49:05:00
Modified: 2020-12-07T07:46:49:05:00
Language: en
Format: x-cmap/x-storable
Publisher: FIHMC CmapTools 6.04
Width: 2534
Height: 1271
Topics
means of authenticating
Password
Authentication
Countermeasures
Authentication Process
something the individual knows
something the individual does
something the individual possess
something the individual is
Policies against similar passwords on network devices
Policies to inhibit users from selecting common passwrods
Account lockout mechanisms
Training and enforcement of password policies
Automatic workstation logout
characteristic
validation for user
Steps
example
example
example
example
ways to provide confidentiality to user id/password
Selection Technique
Proactive Checking
Rule Enforcement
Password Cracking
Vulnerabilities
Offline dictionary attack
Electronic monitoring
widely used line of defense against intruders
user provides name/login and password
id
Verification
Identification
password, PIN, answers to prearranged questions
voice pattern, handwriting, typing rhythm
smartcard, electronic keycard, phyiscal key
fingerprint, retina, face
Hashing
Increases the difficulty of offline dictionary attacks
Controls to prevent unauthorized to password file
Rapid reissuance of compromised passwords
Intrusion detection measures
????
traits
defined
attacks
examples
defined
defined
attributes
attributes
Defined
Defined
Purpose of Salt
Computer generated passwords
Reactive password checking
User Education
Password cracker
Bloom filter
user is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it
goal is to eliminate guessable passwords while allowing the user to select a password that is memorable
specific rules that passwords must adhere to, such as all passwords must be at least eight characters long
Rainbow table
pre-compute tables of hash values of possible passwords combined with all possible salts (of certain length)
Dictionary
Each password must be hashed using each salt value and then compared to stored hash values
Workstation hijacking
Password guessing against single user
Exploiting multiple password use
Exploiting user mistakes
Specific account attack
Attacker obtains the system password file and compares the password hases against hashes commonly of used passwords
If a password is communicated across a network to log on to a remote system, it is vulnerable to eavesdropping
system compares password with the one stored for that specified login
used in discretionary access control
determines the user's privileges such as root or guest
determines that the user is authorized to access the system
Presenting or generating authentication information that corroborates the binding between the entity and the identifier
Presenting an identifer to the security system
Prevent duplicate passwords from being visible in the password file
Difficult to find out whether a person has used the same password on two or more systems
defined
defined
defined
defined
defined
traits
traits
defined
defined
defined
defined
defined
traits
users have trouble remembering them
system periodically runs its own password cracker to find guessable passwords
users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords
compile a large dictionary of bad passwords
efficient way to find a user password in a rejecting words lists
can be countered by using a sufficiently large salt value and a sufficiently large hash length
a mammoth table of hash values
Develop a large dictionary of possible passwords and try each against the password file
The attacker waits until a logged-in workstation is unattended
The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password
Attacks can also become much more effective or damaging if different network devices share the same or a similar password for a given user
If the system assigns a password, then the user is more likely to write it down because it is difficult to remember
Attacker guesses password until the correct password is discovered
Salt changes the hash values of same password