

Evaluating Alternatives to Passwords

Bruce K. Marshall, CISSP, IAM
Senior Security Consultant
bmarshall@securityps.com



■ ■ ■ ■ Key Presentation Topics

- Authentication Model
- Authenticator Characteristics
- Knowledge Based Authenticators
- Possession Based Authenticators
- Biometric Based Authenticators

Identification

- A process for presenting an identity for use.

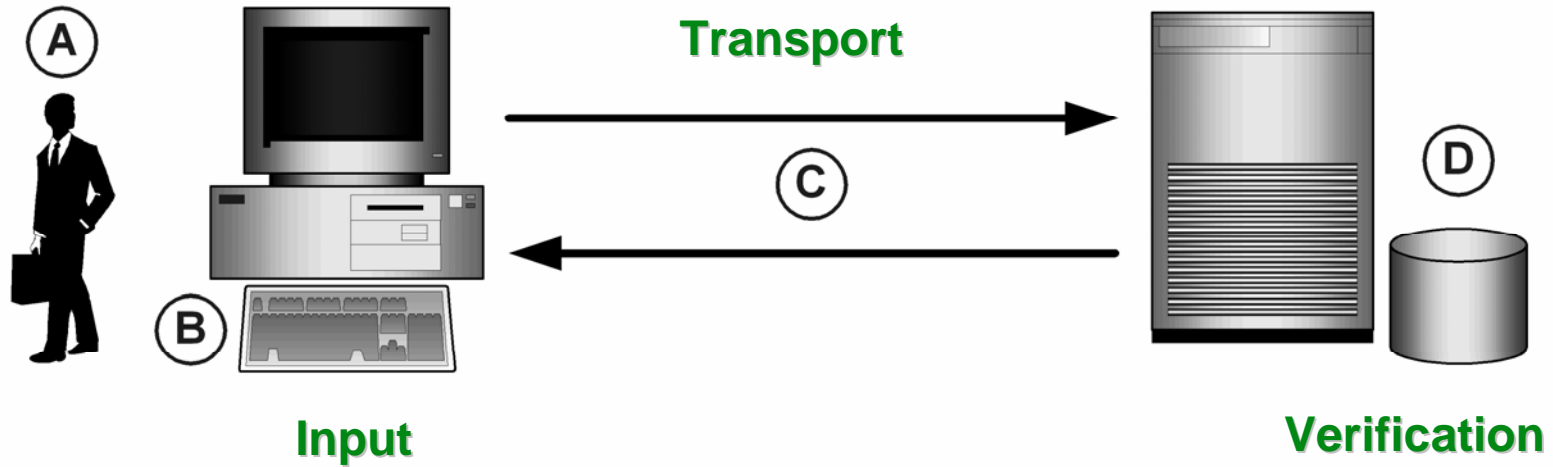
Authentication

- A process for validating proof of an identity.



Authentication System Model

Authenticator



What you know

- Passwords
- Passphrases
- Secret Answers
- Graphical Passwords

What you have


- ID Cards
- Password List
- One-Time Password Tokens
- Private Keys (Certificates)

What you are

- Physical Features
- Psychological Traits



Authenticator Characteristics

- Usability
 - How effectively can people operate
 - Uniqueness
 - How distinct is the proof
 - Integrity
 - How difficult to guess, forge, or steal
 - Affordability
 - How much does it cost to buy or maintain
 - Accuracy
 - How often do mistakes occur
- 



Personal Identification Number (PIN)

- Very simple authenticator
- Difficult to enforce hard-to-guess PINs
- May include non-numeric characters



Secret Answers

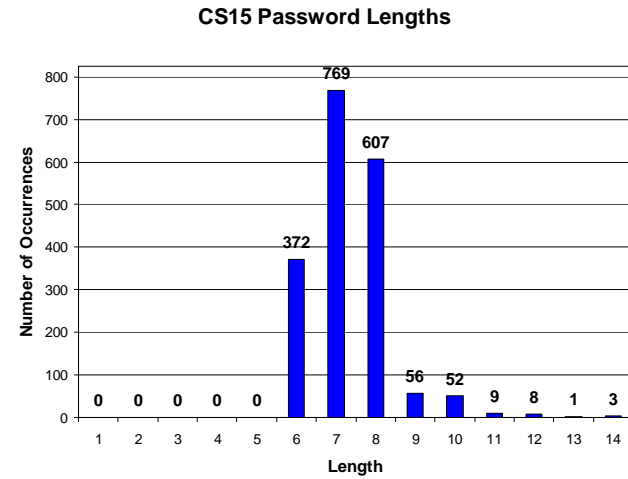
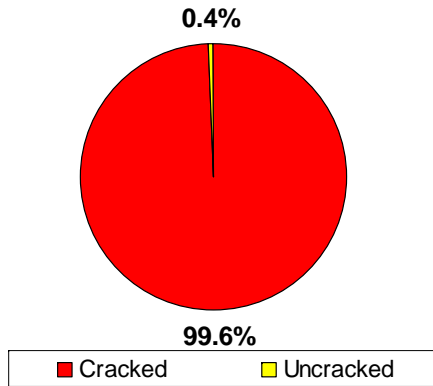
- One or more correct answers authenticates an asserted identity
- Users may be allowed to define questions
- Typically a secondary authenticator



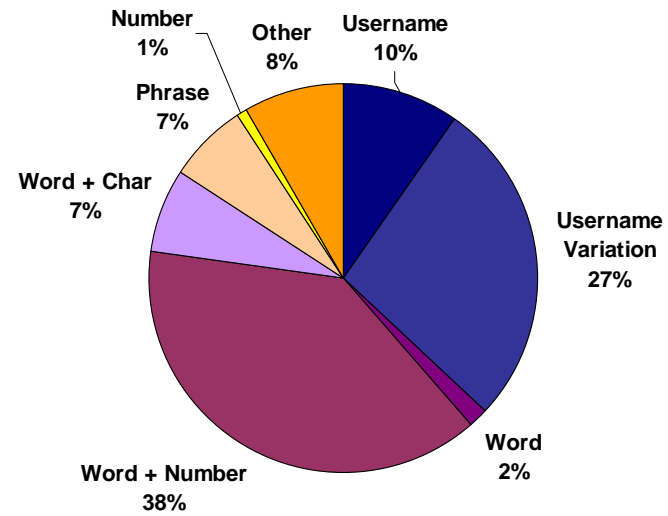
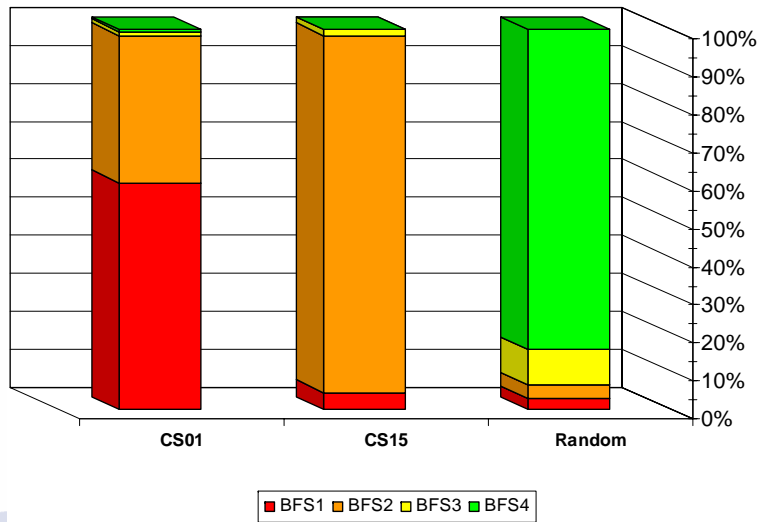
■ Passwords

- Based on a string of characters
- Usually too predictable (i.e. poor uniqueness)
 - Length rarely greater than 8 characters
 - Often consist of words or names
 - Typically composed of lowercase letters
 - Often think alike when choosing passwords
 - Use same password across systems
 - Not changed frequently enough
- Controlled through requirements for character use, length, and pattern matching

Case Study 15 Password Analysis



Cracking Success of L0phtCrack Brute Force Strings



Password Characteristics

Poor Fair OK Good Excellent

Usability



Uniqueness



Integrity



Affordability



Accuracy





Passphrases

- Multiple words, typically mixed case with numbers and symbols
- Improvement upon passwords with little user learning curve
- Not much study yet on predictability

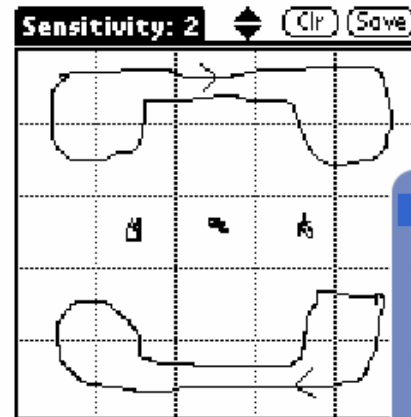
“The light of the M00N struck me in June”

“SeattleSeahawksSingSadSongS4ME”

“emmyis7”

Graphical Passwords

- Rely on memory of images to authenticate
- Users select, draw, or manipulate pictures
- Relatively young technology that needs more attention



“What You Have” Authenticators

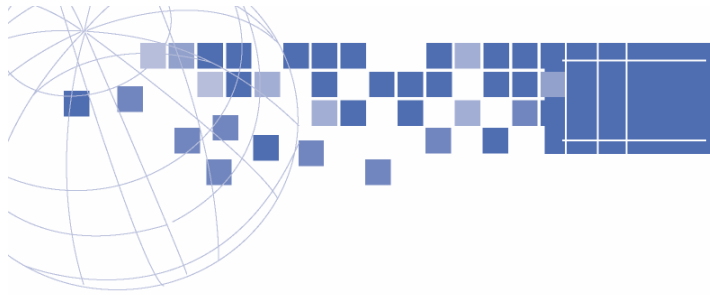
“What You Have” Authenticators

- Magnetic-stripe cards
- RF & Wiegand cards
- Stored-value cards
- Password lists



- One-Time Password (OTP) Tokens
 - Generates a new password for each use
 - Can be challenge/response-based
 - Based on a unique, secret token seed value (and usually synchronized time)
 - Implemented with hardware or software





OTP Tokens Characteristics



Poor

Fair

OK

Good

Excellent

Usability



Uniqueness



Integrity



Affordability

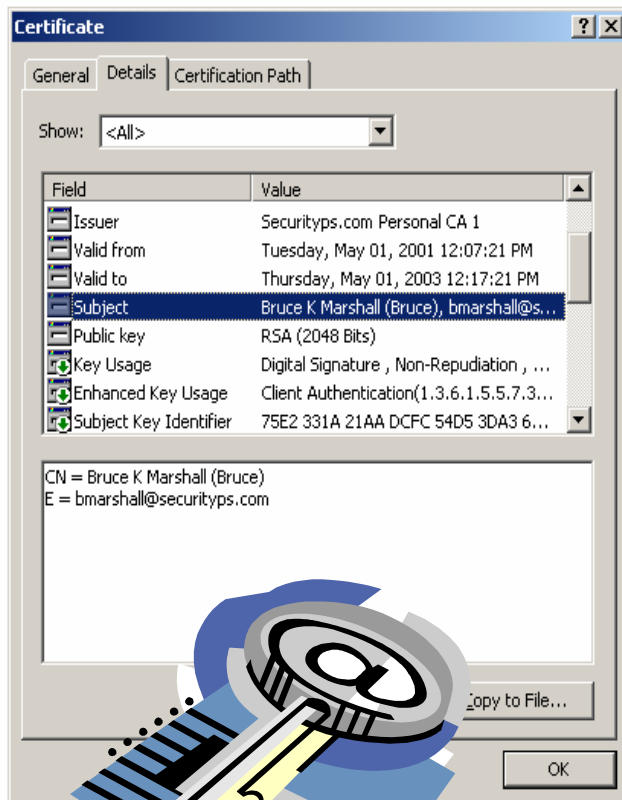


Accuracy



Digital Certificates

- Rely on the use of private and public keys
- Typically require a Public Key Infrastructure (PKI) for certificate creation, publication, renewal, & revocation





Digital Certificate Characteristics

Poor Fair OK Good Excellent

Usability



Uniqueness



Integrity



Affordability

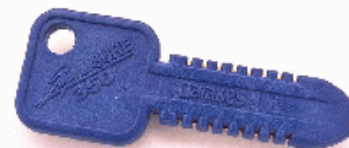
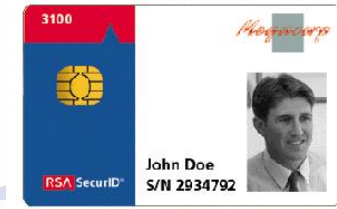
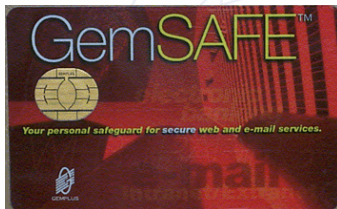


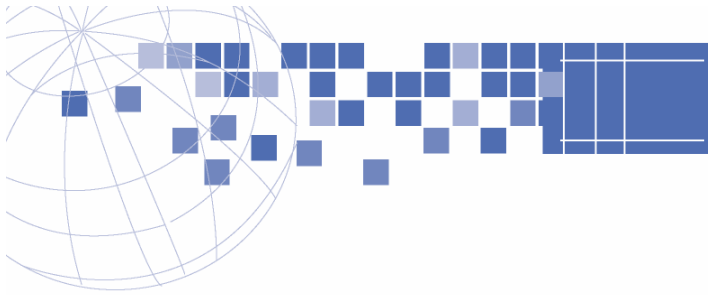
Accuracy



Smart Cards

- Microprocessor with memory that can generate and store keys and certificates
- Different form factors and interfaces
- Cryptographic functions using private key are processed on the card itself





Smart Card Characteristics



Poor

Fair

OK

Good

Excellent

Usability



Uniqueness



Integrity



Affordability



Accuracy



SECURITY PS

STRATEGIC INFORMATION SECURITY

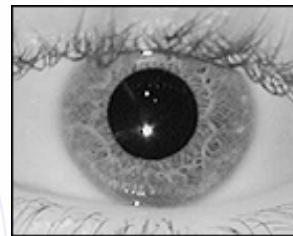


■ ■ ■ ■ Biometric Authenticators

- “The automated use of physiological or behavioral characteristics to determine or verify identity.” – International Biometrics Group
- Rely on interpretation or ‘minutiae’ of a biometric trait
- Maturing technology and standards
- Increasingly used for physical security

Biometric Authenticators

- Fingerprint = 48%
- Face = 12%
- Hand = 11%
- Eye (Iris) = 9%
- Voice = 6%
- Keyboarding = <1%



* - Data source: International Biometrics Group 2004 Market Share

Biometric Characteristics

Poor

Fair

OK

Good

Excellent

Usability



Uniqueness



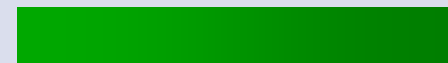
Integrity



Affordability



Accuracy



Multi-Factor Authenticators

- Stronger authentication?
- Can combine best features
- Might combine worst features
- Do not want an Ident-I-Eeze”*



* Coined by Douglas Adams in his book Mostly Harmless.



Summary & Call to Action

- Focus on entire authentication system
- Evaluate suitability of authentication solutions for your specific environment
- Do consider the Integrity of authenticators, but don't forget about other characteristics
- Assess & fortify password dependent systems
- Visit www.passwordresearch.com

Questions?



SECURITY PS

STRATEGIC INFORMATION SECURITY