NIST E-Authentication Guidance: Can we add KBA?

NIST KBA Symposium
Feb. 9, 2004

Bill Burr
william.burr@nist.gov

NIST E-Authentication Tech Guidance

- OMB Guidance to agencies on E-Authentication
  - OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, Dec. 16, 2003
    - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
  - About identity authentication, not authorization or access control
- NIST SP800-63: *Recommendation for Electronic Authentication*
  - Companion to OMB e-Authentication guidance
  - Draft for comment at: http://csrc.nist.gov/eauth
  - Comment period ends: March 15
  - Covers conventional token based remote authentication
    - Does not cover Knowlege Based Authentication (KBA)

Assurance Levels

- OMB guidance defines 4 assurance levels
  - Level 1 little or no confidence in asserted identity's validity
  - Level 2: Some confidence in asserted identity's validity
  - Level 3: High confidence in asserted identity's validity
  - Level 4: Very high confidence in asserted identity's validity
- Needed assurance level determined *for each type of transaction* by the risks and consequences of authentication error with respect to:
  - Inconvenience, distress & damage to reputation
  - Financial loss
  - Harm to agency programs or reputation
  - Civil or criminal violations
  - Personal safety

Technical Guidance Constraints

- Technology neutral (if possible)
  - Required (if practical) by e-Sign, Paperwork Elimination and other laws
  - Premature to take sides in web services wars
  - Difficult: many technologies, apples and oranges comparisons
- Practical with COTS technology
  - To serve public must take advantage of existing solutions and relationships
- Only for remote network authentication
  - Not in person, therefore not about biometrics
- Only about identity authentication
  - Not about attributes, authorization, or access control
    - This is inherited from OMB guidance
  - Agency owns system & makes access control decisions

Personal Authentication Factors

- Something you know
  - A password
- Something you have: a token
  - for remote authentication typically a key
    - Soft token: a copy on a disk drive
    - Hard token: in a special hardware cryptographic device
- Something you are
  - A biometric
    - But biometrics don't work well in remote authentication protocols, because you can't keep a biometric secret

Remote Authentication Protocols

- Conventional, secure, remote authentication protocols all depend on proving possession of some secret “token”
- Remote authentication protocols assume that you can keep a secret
  - Private key
  - Symmetric key
  - Password
- Can be “secure” against defined attacks if you keep the secret
  - Amount of work required in attack is known
  - Make the amount of work work impractically large
  - Hard for people to remember passwords that are “strong” enough to make the attack impractical

Multifactor Remote Authentication

- The more factors, the stronger the authentication
- Multifactor remote authentication typically relies on a cryptographic key
  - Key is protected by a password or a biometric
  - To activate the key or complete the authentication, you need to know the password, or poses the biometric
  - Works best when the key is held in a hardware device (a “hard token”)
    - Ideally a biometric reader is built into the token, or a password is entered directly into token

E-Authentication Model

- A *claimant* proves his/her identity to a *verifier* by proving possession of a *token*, possibly in conjunction with *electronic credentials* that bind the identity and the token. The verifier may then inform a relying party of the claimant's identity with an *assertion*. The claimant got his/her token and credentials from a *Credentials Service Provider (CSP)*, after proving his identity to a *Registration Authority (RA)*. The roles of the verifier, relying party, CSP and RA may be combined in various combinations.
  - ***Claimant:*** Wants to prove his or her identity
  - ***Electronic credentials****:* Bind an identity or attribute to a token or something associated with a claimant
  - ***Token:*** Secret used in an authentication protocol
  - ***Verifier:*** verifies the claimant's identity by proof of possession of a token
  - ***Relying party:*** Relies on an identity
  - ***Assertion:*** *Passes information about a claimant from a verifier to a relying party*
  - ***Credentials Service Provider (CSP):*** Issues electronic credentials and registers or issues tokens
  - ***Registration Authority (RA):*** Identity proofs the subscriber

Tokens

- Hard token
  - Cryptographic key in a hardware device
  - FIPS 140 level 2, with level 3 physical security
  - Key is unlocked by password or biometrics
- Soft token
  - Cryptographic key encrypted under password
  - FIPS 140 Level 1 or higher crypto module
- One-time password device (1TPD)
  - Symmetric key in a hardware device with display - FIPS 140 level 1
  - Generates password from key plus time or counter
  - User typically inputs password through browser
- Zero Knowledge Password
  - Strong password used with special “zero knowledge” protocol
- Password
  - Password or PIN with conventional protocol

Token Type by Level

	Assurance Level			
Allowed Token Types	1	2	3	4
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
Zero knowledge password	√	√	√	
One-time Password Device	√	√	√	
Strong password	√	√		
PIN	√			

Protections by Level

	Assurance Level				
Protection Against	1	2	3		4
			Soft/ZKP	1TPD	
Eavesdropper		√	√	√	√
Replay	√	√	√	√	√
On-line guessing	√	√	√	√	√
Verifier Impersonation			√	√	√
Man-in-the-middle			√	*	√
Session Hijacking			√		√

*** Protection for shared secret only**

Auth. Protocol Type by Level

	Assurance Level			
Authentication Protocol Types	1	2	3	4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Zero knowledge password	√	√	√	
Tunneled password	√	√		
Challenge-reply password	√			

ID Proofing

- Level 1
  - Self assertion, minimal records
- Level 2
  - On-line, more or less instant gratification may be possible
    - Close the loop by mail, phone or (possibly) e-mail
- Level 3
  - in-person registration not required
    - Close the loop by mail or phone
- Level 4
  - In person proofing
    - Record a biometric
      - Can later prove who got the token
  - Consistent with FICC Common Certificate Policy

PKI & E-Auth

- PKI solutions widely available
  - Can use TLS with client certs. for levels 3 & 4
- May be the predominant solution for levels 3 & 4 in gov.
  - Federal Identity Credentialing Committee
  - Common Credential and Federal Identity Card
    - Common certificate policy and shared service providers
    - Gov. Smart Card Interoperability Standard (GSC-IS)
- Fed. Bridge CA and Fed. Policy Authority are PKI vehicle
- Non-PKI level 3 & 4 solutions
  - One-time password devices in common use – can meet level 3
    - Cell phones could be a good 1TPD platform
  - Zero knowledge passwords for level 3 – not widely implemented
  - Level 4 could be done with symmetric key tokens

Passwords

- Password is a secret character string you commit to memory.
  - Secret and memory are the key words here
    - As a practical matter we often do write our passwords down
- A password is really a (weak) key
  - People can't remember good keys
- We all live in Password Hell – too many passwords
  - And they try to make us change them all the time
- In E-auth we're only concerned with on-line authentication
  - Assume that the verifier is secure and can impose rules to detect or limit attacks
- What is the "strength" of a password?

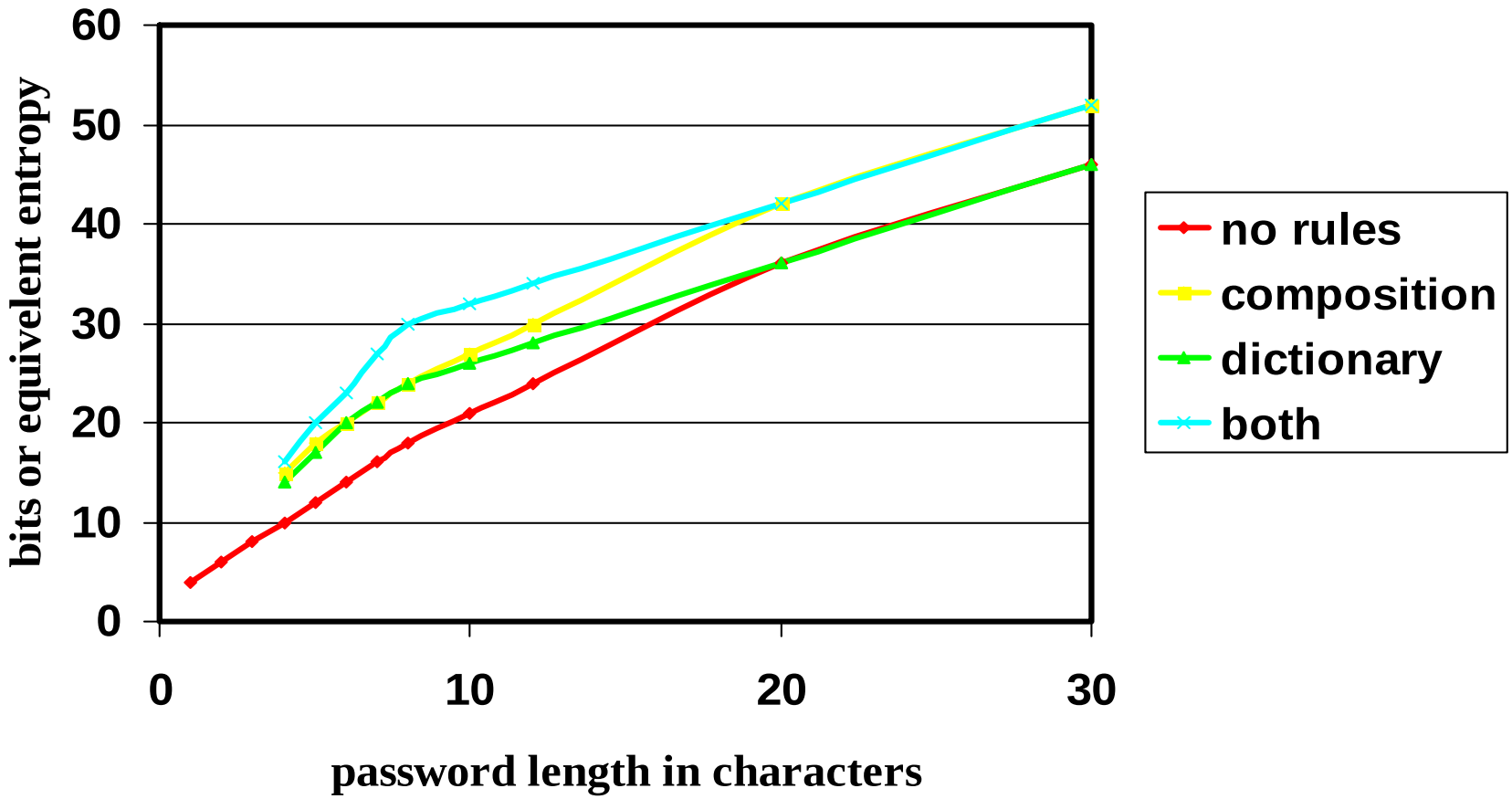
Password Strength

- Over the life of the password the probability of an attacker with no *a priori* knowledge of the password finding a given user's password by an in-band attack shall not exceed
  - one in 2^{16} (1/65,563) for Level 2
  - one in 2^{11} (1/2048) for Level 1
- Strength is function of both password entropy & system
- Many ways to limit password guessing attack
  - 3-strikes and reset password, hang up on bad login attempt…
  - Limited password life, but…
  - Note that there is not necessarily a time limit
  - Many things are trade-offs with help desk costs

Password Entropy

- Entropy is measure of randomness in a password
  - Stated in bits: a password with 24 bits of entropy is as hard to guess as a 24 bit random number
  - The more entropy required in the password, the more trials the system can allow
- It's easy to calculate the entropy of a system generated random password
  - But users can't remember these
- Much harder to estimate the entropy of user chosen passwords
  - Composition rules and dictionary rules may increase entropy
  - NIST estimates of password entropy

Very Rough Password Entropy Estimate



NIST
National Institute of Standards and Technology

Knowledge Based Authentication (KBA)

- Can we just ask questions to authenticate users?
  - People do it now
  - "Walk-in" customers, real business need
    - It's the age of instant gratification
- Similar to ID proofing process, but without closing the loop
- Could view KBA as similar to passwords
  - Only these passwords are not very secret
  - Valid claimant might not know them all
- How can we quantify KBA, what are the standards?

KBA: some questions

- What is a reasonable model for KBA?
  - What are the functions and features of each component?
  - What are the security implications of the components?
- For Users:
  - How much confidence do you need? Can KBA get there?
- What are the information sources and how do we evaluate them?
  - How accurate are the sources?
- What are the Mechanisms and Metrics?
- How do we score responses and what does a score mean?
- What can we standardize?

Questions