NIST E-Authentication Guidance SP 800-63

Federal PKI Deployment Workshop
May 19, 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 ended: March 15
  - Covers conventional token based remote authentication
    - Does not cover Knowledge Based Authentication

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

E-Auth Guidance Process

- Risk assessment
  - Potential impacts
  - likelihood
- Map risks to assurance level
  - profile
- Select technology
  - NIST Technical E-Authentication Guidance, SP800-63
- Validate implemented system
- Periodically reassess

Max. Potential Impacts Profiles

Potential Impact Categories for Authentication Errors	*Assurance Level Impact Profiles*			
	1	2	3	4
Inconvenience, distress, reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency prog. or pub. interests	N/A	Low	Mod	High
Unauth. release of sensitive info	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

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
    - But SAML looks like it's here to stay
  - 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
  - FICC is addressing credentials for building access for Fed. Employees and associates
- Only about identity authentication
  - Not about attributes, authorization, or access control
    - This is inherited from OMB guidance
  - Agency owns application & 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: key in a special hardware cryptographic device
- Something you are
  - A biometric

NIST
National Institute of Standards and Technology

Remote Authentication Protocols

- Conventional, secure, remote authentication protocols all depend on proving possession of some secret “token”
  - May result in a shared cryptographic session key, even when token is a only password
- 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
  - Work required for attack can be calculated or estimated
    - Make the amount of work impractical
  - Often hard for people to remember passwords that are “strong” enough to make the attack impractical

Biometrics

- Biometrics tie an identity to a real person
- Biometrics don't make good secrets for conventional remote authentication protocols
  - Hard to keep them secrets
  - Limited number per person
  - Can't change or revoke them
    - This is a feature, not a bug, it's why biometrics are so useful
- Biometric authentication doesn't depend on keeping it secret, it depends on being sure that it is a fresh, true biometric capture
  - Easy when the person is standing in front of you at the capture device
  - Hard when all you have is bits coming from anywhere on the internet.
  - 800-63 makes limited use of biometrics
  - NIST expects to hold a workshop on biometrics & remote authentication in the fall

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

NIST
National Institute of Standards and Technology

E-Authentication Token Model

- A *claimant* proves his/her identity to a *verifier* by proving possession of a *token*, often 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 variously combined in one or more entities.
  - ***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	√			

NIST
National Institute of Standards and Technology

Protections by Level

	Assurance Level			
Protection Against	1	2	3	4
Eavesdropper		√	√	√
Replay	√	√	√	√
On-line guessing	√	√	√	√
Active network attacks			√	√
Malicious host software				√

NIST
National Institute of Standards and Technology

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 – Three Questions

- Is Joe Blow real person? Does a person named Joe Blow with the claimed attributes exist?
  - As a practical matter, if somebody lives for a while under a name, that person exists
- Is the applicant that Joe Blow?
- Can Joe Blow later repudiate his registration?
  - Can Joe later say, “Look, you may have registered somebody as Joe Blow, but it wasn’t me.”

ID Proofing – is Joe Blow a real person?

- Database entries
  - Employment records, school records, credit records, voter rolls, tax records, DMV…
    - Can't easily get access to some databases
- Relationship and history with some organization
  - School, employer, bank (know your customer), business customer…
- Paper credentials
  - Drivers License, Agency ID, Birth Certificate, Passport
    - Are the credentials confirmed by the issuer?
      - Could be forgeries
    - Generally requires in-person appearance at RA

ID Proofing – is this the real Joe Blow?

- In-person Picture ID
  - compare applicant to Joe's photo
- But, in-person registration is often expensive and inconvenient
  - Compromise
    - Make the applicant prove he/she knows a lot about Joe
    - Close the loop: Make the applicant prove that he/she can get mail, make a call or get e-mail at an address associated with Joe in the records

ID Proofing – can Joe repudiate registration?

- In-person Picture ID
  - Keep a copy of Joe's picture ID
  - Better yet take Joe's picture (or signature, fingerprint, etc.)
- But, in-person registration is often expensive and inconvenient
  - Compromise
    - Make the applicant prove he/she knows a lot about Joe Blow, an impostor at least had to do his homework
    - Close the loop: Make the applicant prove that he/she can get mail, make a call or get e-mail at an address associated with the claimed identity in the records – an impostor, if there was one at least had access to Joe's address of record
    - Record a voice at a phone number of record

ID Proofing

- Level 1
  - Self assertion, minimal records
- Level 2
  - Remote or in-person; Modeled after OCC “know your customer” rules for banks
    - In person: visual inspection of primary gov. photo-ID
    - Remote: supply numbers for primary gov. ID and financial account number with records confirmation of one
    - Notification to address of record
- Level 3
  - Remote or in-person
    - In person: present gov photo-ID, confirm ID with issuer or other records, confirm address ofrecord with ID or issuance process
    - Remote: supply numbers for primary gov. ID and financial account number with records confirmation of one and confirm address of record
- Level 4
  - In person proofing only
    - 2 ID’s or database records, must confirm at least one
    - Record a biometric
      - Can later prove who got the token

ID Proofing

- At level 2
  - Financial institutions regulated by the OCC can issue credentials for their customers
  - Educational institutions can issue credentials for their students
  - Employers can issue credentials for their employees
- Cert policies
  - Level 2: FBCA basic, Citizen and Commerce Class
  - Level 3: FBCA medium
  - Level 4: FBCA High, Common

Passwords

- Password is a secret (typically a 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?

Attacks on Passwords

- In-band
  - Attacker repeatedly tries passwords until he is successful
    - guessing, dictionary, or brute force exhaustion
  - Can't entirely prevent these attacks
    - can ensure they don't succeed very often
- Out of band – everything else
  - Eavesdropper
  - Man-in-the-middle
  - Shoulder surfing
  - Social engineering

NIST
National Institute of Standards and Technology

In-Band Attacks on Passwords

- Targeted attacks
  - Attacker is trying to find the password of a particular person
  - “Guessing Entropy” is a measure of the difficulty attacker who knows the password frequency distribution has to find the password of a selected user. This attacker will try every password for the selected user in order of decreasing probability.
- Untargeted attacks
  - Attacker is trying to find anybody’s password, doesn’t care who
    - Looks for users with commonly selected passwords
  - “Min entropy” is a measure of how hard it is for an attacker who knows the password frequency distribution to fine any user’s password, we don’t care how. This attacker will try the most common password(s) for all users.

Password Strength – Min Entropy

- Level 1 – no min entropy requirements
- Level 2 passwords must have at least 10 bits of min entropy
  - Two randomly chosen keyboard characters (or 4 passfaces) have at least 12 bits of min entropy
  - We (somewhat arbitrarily) allow that a well chosen dictionary of at least 10,000 not allowed passwords ensures at least 10 bits of min-entropy
  - We (somewhat arbitrarily) allow that an 8 character user selected password containing at least 3 of the 4 kinds of characters (lower case, upper case, numeric & special) ensures at least 10 bits of min entropy
  - Other reasoned arguments for min entropy are permitted
- Level 3 passwords must have at least 12 bits of min entropy
  - We (somewhat arbitrarily) allow that a well chosen dictionary of at least 100,000 not allowed passwords ensures at least 12 bits of min-entropy
  - We (somewhat arbitrarily) allow that an 10 character user selected password containing at least 3 of the 4 kinds of characters (lower case, upper case, numeric & special) ensures at least 10 bits of min entropy
  - Other reasoned arguments for min entropy are permitted

Password Strength

- Untargeted attack mitigation at levels 2 & 3
  - Verifiers must monitor to detect and block repeated unsuccessful authentication attempts from the same address.
- Level 3 – social engineering protection
  - System must include provisions that make it difficult to verbally communicate passwords
    - for example passwords may be based, at least in part, on recognition and selection of complex images, (not easily described verbally) from fields of images
    - other solutions are possible
  - Extensive training of users
- Composite passwords allowed
  - 2 randomly chosen char with user selected
  - Image selection with character string password
  - Entropy adds

Secure Password Client

- For Level 3 use of passwords we require a “secure client”
- Browsers are not considered secure clients
  - Too many trust anchors, too complex, to hard for users to understand and control what is going on, too easy for servers to control what the user sees
- But TLS is a good protocol & SPEKE or EKE or other are good protocols using the right client
- Secure Client
  - Separately invoked directly by user
  - Distinct appearance
  - Must block verifier impersonation attack; either
    - Zero knowledge password protocol or
    - Single trust anchor and not allow user to override server certificate verification

Password Strength – guessing entropy

- 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} (1/65,536) for Level 3
  - one in 2^{14} (1/16384) for Level 2
  - one in 2^{10} (1/1024) for Level 1
- Strength is function of both password guessing entropy, the system and how it limits or throttles in-band guessing attacks
- 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 of a password is roughly speaking, the uncertainty an attacker has in his knowledge of the password, that is how hard it is to guess it.

$$H(X) := -\sum_{x} P(X = x) \log_2 P(X = x)$$

- Easy to compute entropy of random passwords
- We typically state entropy in bits. A random 32-bit number has 2^{32} values and 32-bits of entropy
- A password of length l selected at random from the keyboard set of 94 printable (nonblank) characters has 94^l values and about $6.55 \times l$ bits of entropy.

NIST
National Institute of Standards and Technology

Password Guessing Entropy

- Guessing entropy is measure of randomness in a password
  - Stated in bits: a password with 24 bits of entropy is as hard to guess on average 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 guessing entropy

Shannon's Estimate of Entropy

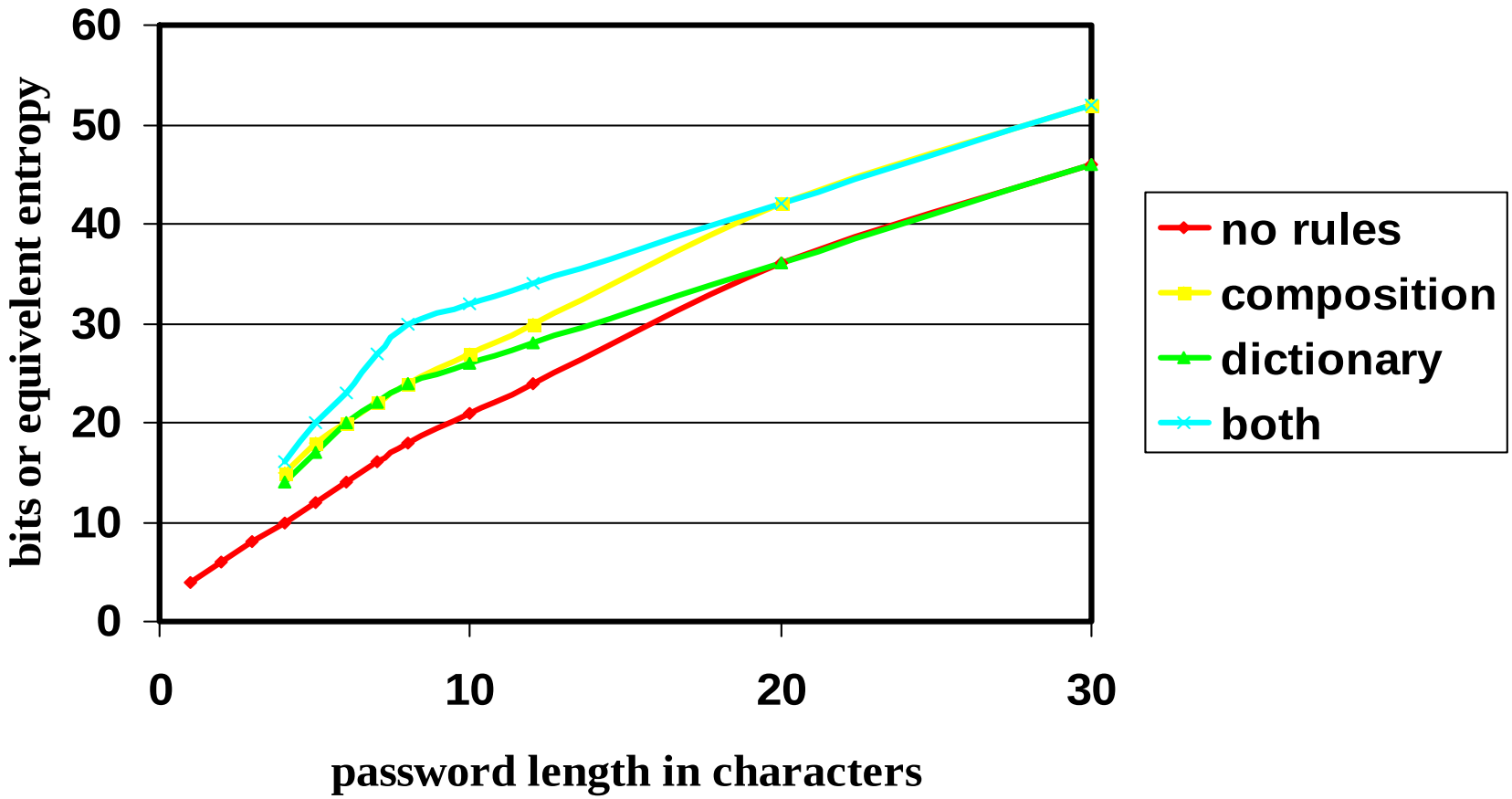
- Shannon used 26 English letters plus space
  - Left to their own devices user will choose only lower case letters.
- Shannon's method involves knowing the *i*-1 first letters of a string of English text; how well can we guess the *i*th letter?
- Entropy per character decreases for longer strings
  - 1 character 4.7 bits/character
  - ≤ 8 characters 2.3 bits per character
  - order of 1 bit/char for very long strings

NIST
National Institute of Standards and Technology

Use Shannon as Estimate

- Shannonn gives us an estimate of the number of bits needed to represent ordinary English text
  - Seems intuitive that if it takes n bits to represent a text string, that is related to how hard it is to guess the string
- It should be as hard to guess or compress passwords as ordinary English text
  - Users are supposed to pick passwords that don't look like ordinary English, to make them harder to guess
    - But, of course, users want to remember passwords
  - Attacker won't have a perfect dictionary or learn much by each unsuccessful trial
  - Surely, the only long passwords that are easy to remember are based on phrases of text that make sense to the person selecting the password
- Give "bonuses" for composition rules and dictionary

Rough Password Guessing Entropy Estimate



NIST
National Institute of Standards and Technology

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

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
    - OATH – USB tokens
    - 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

FPKI Certificate Policies

- Federal Certificate Policy
  - Rudimentary, Basic, Medium and High
  - Federal Policy Authority “maps” agency policy
  - currently x-certified
    - Medium: Treasury, DoD, Agriculture (NFC), NASA, DST ACES, Illinois
    - High: State Dept & Treasury
- Common Certificate Policy
  - Shared Service providers
- Citizen and Commerce Class
  - Streamlined process based on memo of agreement rather than detailed review of CP & CPS
    - Does anybody want this?

Knowledge Based Authentication (KBA)

- Not covered in 800-63
  - Symposium on 9-10 Feb. at NIST
- 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 Merchant use

- Service provider gives merchant a score, the higher the score, the better risk the customer is.
  - Scoring method is proprietary
- Merchant picks a score threshold
  - Threshold is too high, turn away good business
  - Threshold to low, too many bad transactions
- Merchant adjusts threshold to maximize profits.
  - Clear feed back metric: profits
- How do we translate this into man government applications where major concern is not profit, but privacy?

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