

# NIST E-Authentication Guidance SP 800-63 and Biometrics

September 21, 2004

Bill Burr  
william.burr@nist.gov

# OMB M-0404 Guidance on E-Auth

- Part of E-Government initiative – put services online
- About identity authentication, not authorization or access control
- <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- Four 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 consequences of authentication error with respect to defined potential impact categories

# Max. Potential Impacts Profiles

<i>Potential Impact Categories for Authentication Errors</i>	<i>Assurance Level Impact Profiles</i>			
	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

# 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

# NIST SP800-63: Electronic Authentication Guideline

- A NIST Recommendation
- Companion to OMB e-Authentication guidance M-0404
  - Provides technical authentication requirements for levels of authentication assurance defined in M-0404
- Posted end of June 04
  - [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6\\_3\\_3.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf)
- Covers conventional secret token based remote authentication
  - Does not cover Knowledge Based Authentication
  - Modest use of biometrics in registration & to unlock keys
- Fairly well received by network security professionals and cryptographers

# Technical Guidance Constraints

- Technology neutral (if possible)
  - Required (if practical) by e-Sign, Paperwork Elimination and other laws
  - Don't want 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
  - Other efforts for Fed. Employees/associates credentials for building access
  - 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

# 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 only a password
- Remote authentication protocols assume that you can keep a secret
  - Private key, Symmetric key or 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
  - People can’t remember passwords strong enough to make “offline attacks” impractical
  - Good password remote authentication blocks eavesdropper attacks
    - Harder to prevent shoulder surfing or phishing

# Multifactor Remote Authentication

- The more factors, the stronger the authentication
  - Two factors required for Level 3 by 800-63
- 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 possess 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
- Are there other ways?
  - Not yet in 800-63

# Biometrics

- Biometrics tie an identity to a human body
- Biometric authentication depends on being sure that you have a fresh, true biometric capture, not on keeping the biometric secret
  - 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
  - NIST plans a workshop on biometrics & remote authentication in the winter
- Biometrics aren't suitable secrets for remote authentication protocols
  - Hard to keep them secrets
  - Limited number per person
  - Can't change them
    - This is a feature, not a bug, it's why biometrics are so useful
    - Maybe you could revoke them, but would you like the process?

# Culture Clash

- Current remote authentication methods are mainly cryptographic
- Cryptographers are adversarial
  - Propose a new crypto method and everybody tries to break it
  - Kerchoffs assumption: an adversary will know all the details of the design of your system (only secrets are operational keys)
- Cryptographers will develop an attack and publish it in enough detail so that others can replicate their work, and think they have done a good thing
  - 5 hash algorithms including MD5 publicly broken at crypto 2004
  - Fluhrer/Shamir RC4 papers lead to WEPCrack & AirSnort “kiddie scripts”
  - We do this to crypto & we’ll do it to biometrics authentication too
    - Cryptographers believe that a dental technician has the skills and materials to construct a copy of a fingerprint that will fool most fingerprint readers
- Can biometrics stand up to this kind of public, sustained attack?

# Some Workshop Issues

- We have the model of building a biometric reader into a personal cryptographic token to unlock the user's key in 800-63 now
  - How else can we get strong remote authentication with biometrics?
- What are acceptable false acceptance rates and how can we measure them?
- Can we get Level 2 with only a biometric factor?
  - Can we get to  $2^{-14}$  false acceptance rates?
- Can we combine a password and a biometric to get to Level 3?
- For crypto tokens we have FIPS 140 validation testing: how do we get the biometric equivalent?
- How can a remote verifier know it has a fresh “real” biometric?
  - Not an old copy of a biometric and not something synthesized
- What are the privacy implications of large biometric databases?
- What is the process for working on this?

# Questions

---

