

Biometrics and Electronic Authentication

September 20, 2005

Bill Burr
william.burr@nist.gov

Authentication: Local vs Remote

● Local authentication

— Verifier can control & supervise entire process

- Claimant may be supervised (to various degrees) or unsupervised
- Verifier knows where claimant physically is

● Remote authentication

— Verifier control and supervision is harder

- Claimant generally uses his own system, controls his own software
- Claimant is generally unsupervised
- Verifier usually knows only that claimant has network access

Personal Authentication Factors

- **Something only you should know**
 - Typically some kind of password
- **Something only you should have**
 - For local authentication typically an ID card
 - For remote authentication typically a cryptographic key
 - “hard” & “soft” tokens
- **Something only you are**
 - A biometric
 - Unattended capture is problematic Capture can deter fraud even if not checked in authentication process
- **More factors provide stronger authentication**

Conventional Remote Authentication Protocols

- **Prove possession or knowledge of some secret “token”**
 - May result in a shared cryptographic session key, even for passwords
- **Assume that you can keep a secret**
 - Private key, Symmetric key or Password
 - Isn't much of security mainly about keeping secrets?
- **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

Remote Authentication Attacks

- **Eavesdropper** – listens in
 - Only matters to authentication validity if mechanism is based on a secret
 - But we tend to think of biometrics as “private”
 - Is this only because we try to use biometrics as secrets?
 - I argue it’s deeper than that
- **Social Engineering** – attacker persuades user to do something insecure
 - Probably no remote authentication method is entirely immune
 - User training can help
- **Malware & intrusion** – bad software introduced on claimant’ computer
 - Copied token: some tokens are easy to copy & the user won’t know
 - Hardware crypto tokens can protect the a crypto key itself but still usually can be exploited by host systems malware
 - Hard to imagine a user workstation remote authentication technology that is entirely immune, but trusted computing platforms could help

Remote Authentication Attacks

- **Decoys and Phishing**

- Impersonate a real site and either facilitate a man-in-the-middle attack or simply capture passwords or biometrics for replay or later use
- Phishing brings victim to the decoy
- Greatly facilitated by bad browser user interfaces that give host systems too control of what the user sees.

- **Man-in-the-middle (MITM)** – live communications go through the attacker to real host system

- Can be started by phishing or various kinds of decoys
- Can allow attacker to simply eavesdrop, or can allow session hijacking
- Some cryptographic protocols are immune
 - Need to be sure that your browser is really running the protocol you think it is with the right trust anchors
- Live on-line attacks are harder to do than simple decoys

OMB M-04-04 & NIST SP 800-63

● **OMB M-04-04 Policy Guidance for e-authentication**

- Agencies classify electronic transactions into 4 levels needed authentication assurance according to the potential consequences of an authentication error
 - Consider: privacy, inconvenience, damage to reputation, harm to agencies and programs, financial liability, crime, safety

● **NIST SP 800-63: Technical authentication Framework for remote e-authentication**

- <http://csrc.nist.gov/publications/nistpubs/index.html>
- Establishes technical requirements for 4 levels of M0404 for
 - Identity proofing requirements
 - Authentication protocols and mechanisms based on secrets

Multifactor Remote Authentication

- **The more factors, the stronger the authentication**
 - Two factors required for Level 3 by 800-63
- **Multifactor remote authentication typically uses a crypto 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

Four technology levels of SP 800-63

● Level 1 (little confidence in asserted identity)

- No identity proofing
- Relatively weak passwords allowed; may be vulnerable to eavesdroppers

● Level 2 (some confidence in asserted identity)

- Better passwords, but
 - Single factor & still very vulnerable to phishing, social engineering, etc.

● Level 3 (high confidence in asserted identity)

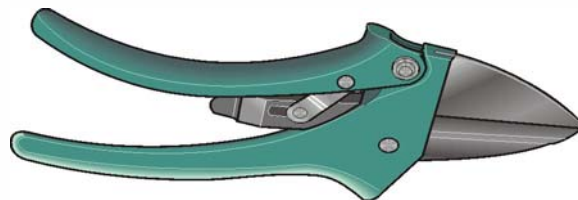
- Two factors,
 - password/biometrics + soft crypto token or one-time password device
 - Phishing attacks shouldn't get master auth. secret

● Level 4 (very high confidence in asserted identity)

- Two factor authentication plus In person ID proofing
- Hard crypto tokens required – something you tangibly have
- Crypto binding of authentication and data transfer
- Protocols block MITM

Biometrics

- **Biometrics tie an identity to a human body**
- **Biometric authentication depends on being having 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
 - Harder if all you have is bits from anywhere on the internet
- **Biometrics aren't suitable secrets for remote authentication**
 - Hard to keep them secrets
 - Limited number per person and you can't change them
 - 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 with Cryptographers

- **Remote authentication methods are mainly cryptographic**
- **Cryptographers are adversarial**
 - Propose a new crypto method and everybody tries to break it
 - Kerchoffs assumption: adversary knows detailed design of your system
 - only secrets are operational keys
- **Cryptographers will develop an attack, publish it so others can replicate their work, and think they have done a good deed**
 - Widely used crypto protocols are broken and methods are published
 - We do this to crypto & we'll do it to biometrics authentication too
- **Can biometrics stand up to this kind of sustained attack?**

Privacy & Biometric Authentication

- Privacy & authentication principle: authenticate an authority or privilege if you can rather than an identity
 - Keys or passwords can represent privileges rather than identities
 - Some protocols guarantee personal anonymity
- Biometrics identify individual people
- It's very hard to revoke and change biometrics
 - That's a feature not a bug
- Much privacy policy angst about on-line files of biometrics
 - Perception matters

Some Personal Conclusions

- **Big advantages to a biometric auth. factor**
 - Direct rather than indirect evidence of personal identity
 - Can't forget or lose biometrics
- **We can manage false acceptance/rejection**
 - Engineering issue: must measure performance and design the overall system accordingly
 - Need security & performance testing comparable to FIPS 140 testing
- **It seems inherently hard to keep a biometric a secret**
 - Shouldn't share an authentication secret with more than 2 parties
- **“Synthetic” attacks don't seem to have been studied much**
 - I would not use real biometrics captures to attack remote authentication, I would synthesize my attack data
- **Privacy is a serious issue**

NIST & INCITS M1 Work

- Held workshop on Biometrics and E-Authentication over Open Networks, March 30 2005
 - <http://www.csrc.nist.gov/pki/BioandEAuth/>
- Formed INCITS M1.4 Ad Hoc Group on Biometrics and E-Authentication to resolve issues
 - Cathy Tilton is chair
 - 1st Meeting June 7, 2005 Cherry Hill, NJ
 - 2nd Meeting Sept. 21, 2005, 1:00-6:00 PM Regency Ballroom B
 - You're all invited

Questions

