



CESG

Threat Analysis

How Can We Compare Different Authentication Methods?

Philip Statham - CESG Biometrics Programme Manager

philip.statham@cesg.gsi.gov.uk

© Crown Copyright. All rights reserved.

Outline

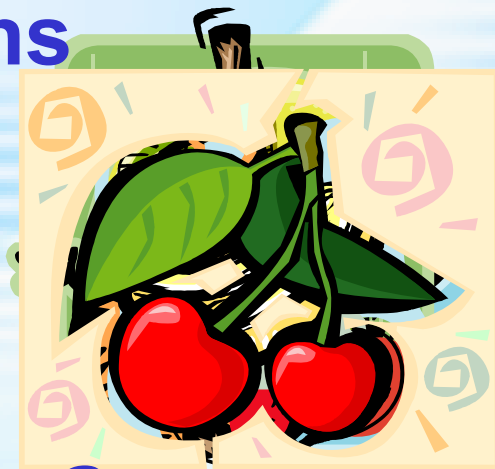
- Authentication mechanisms, parameters and binding
- Strengths and weaknesses of Password, Token and Biometric authentication mechanisms
- Comparing authentication mechanisms
- Combining authentication mechanisms
- CESG biometric authentication policy advice for UK Government

Classic Authentication Paradigm

- *Something you know – Password*
- *Something you have – Token*
- *Something you are – Biometric*

Inevitable Follow-on Questions

- *Which is best?*
- *Which is most secure?*
- *How can we compare them?*



Key Security Issue for all authentication mechanisms is **Binding**

- The confidence you can have that a person presenting the credential is who they claim to be
- What limits the Binding strength?
 - Fundamental – raw entropy of the mechanism
 - Physical linkage of credential to person
 - Procedural/Human weaknesses
 - Technical vulnerabilities of mechanism
- In practice, human and procedural weaknesses often dominate ***Hint: Biometrics helps here***

Threats to Binding Strength

- **Fundamental Discrimination (Entropy) limits**
 - Discrimination, “raw” entropy – ability of mechanism to distinguish between individuals
 - The exploitation avenue for casual (low or zero-effort) attacks
- **Human and procedural failures** – reduces entropy, sometimes to zero
 - Social engineering
 - “Easy” secrets
 - Failure to guard secrets
 - Corrupt users/administrators
- **Technical attacks**
 - Exhaustion attacks against authentication mechanism
 - Exploitation of vulnerabilities of the authentication mechanism
 - Indirect attacks against supporting infrastructure
 - Transmission paths
 - Databases

Security is Multi-Dimensional

Brief Look at the different mechanisms

Passwords

- Discrimination high
 - Large password space – high entropy
- Technically strong
 - Long string = High entropy, very long time to exhaust
 - Cryptographically strong algorithms – can't be reverse engineered
- Procedurally weak
 - Short passwords = Low entropy
 - Easy-to-guess passwords = Low/zero entropy
 - Written down = Zero entropy
 - Divulged to colleagues = Zero entropy
 - Vulnerable to social engineering attacks = Zero entropy
- Password security paradox
 - Increased technical strength ► decreased procedural strength

Tokens

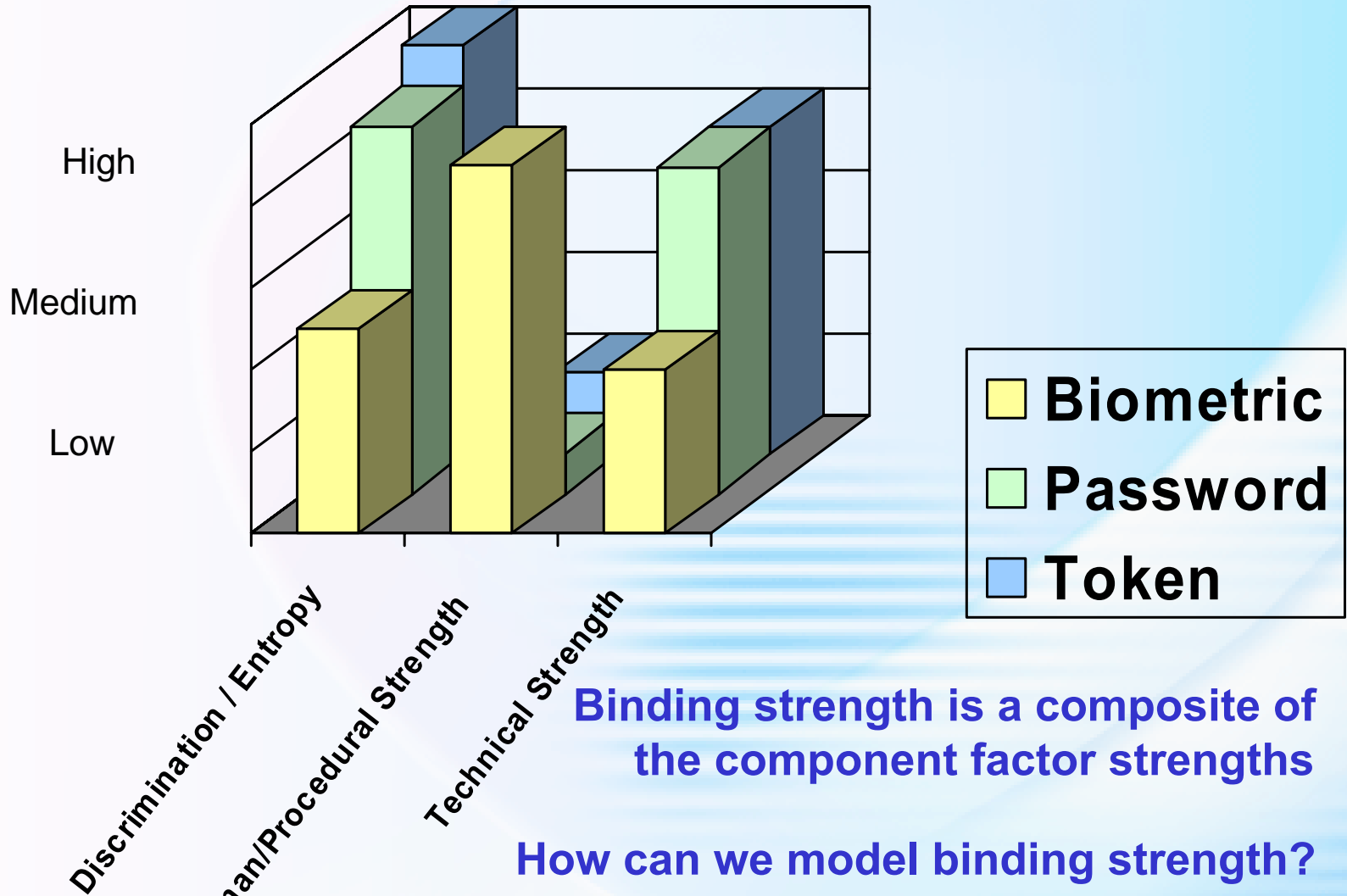
- Discrimination very high – token store “password”
- Technically (quite) strong
 - Difficult to copy – physical barriers
 - very difficult to modify – physical and cryptographic barriers
 - Attacks needs considerable expertise and specialised equipment
- Procedurally weak
 - Loss
 - Theft
 - But at least you know when it’s missing!

Biometrics

- Discrimination medium – high (depending on modality)
 - Entropy limited by FAR
 - N.B. Not directly equivalent to password entropy because you can't mount a simple exhaustion attack
- Technical strength medium
 - Spoofing
 - Reverse engineering of stored templates
 - Capture of stored images
- Procedurally strong
 - Not so reliant on human discipline
 - Human failures don't weaken the binding in the same way as for passwords and tokens



Comparing Authentication Mechanisms



Composite Binding Strength

Model 1: Aggregate the component strengths



Sanity Check: If one component has zero strength, binding strength reduces to sum of other component strengths !!!!!!!

Composite Binding Strength

2nd Model: Aggregate the component weaknesses

$$\text{Weakness} = 1 / \text{Strength}$$



Sanity Check:

If one component has zero weakness (i.e. perfect strength), the overall binding weakness reduces to sum of other component weaknesses

If one component has much greater weakness than the others, it dominates the overall binding weakness

these seem intuitively right.

How do we measure the parameters?

1. Discrimination Strength (Entropy)

Passwords	Raw Entropy/ number of attempts in a defined time period
Tokens	Number of distinct tokens
Biometrics	FAR / number of different attempts feasible.

How do we measure the parameters?

2. Technical Strength

Passwords	Assess through security evaluation process. Results expressed in quantised levels (EALs, or some other scale)
Tokens	
Biometrics	

How do we measure the parameters?

3. Procedural Strength

Hard. May depend on environmental factors such as site security and staff discipline. After the fact audit?

Factors Include:

Passwords	length, randomness, physical security, frequency of change, enforcement policy, user discipline, no of users.
Tokens	physical security, user discipline, no of users
Biometrics	Inherently good, maybe can disregard?

Example

Compare Password and Biometric “Strength of Function” through consideration of entropy

Password SOF

- SOF relates to probabilistic mechanisms
- For passwords this maps to the probability of guessing the password
 - Password SOF defined by entropy
 - e.g. 4 digit PIN has raw entropy of 10000
 - Real entropy may be less (restricted subsets, non random choice etc.)
 - Also effective entropy reduced by multiple attempts

Password Entropy

NIST Special Publication 800-63 – Electronic Authentication Guideline

Table A.1 – Estimated Password Guessing Entropy in bits vs. Password Length

Length Char.	User Chosen			Randomly Chosen		
	94 Character Alphabet			10 char. alphabet		94 char alphabet
	No Checks	Dictionary Rule	Dict. & Comp. Rule			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4



Biometric Entropy and Password Equivalence

- Biometric authentication has a probability of chance (false) match, given by the FAR
- So we infer that biometric entropy is related to FAR (for authentication)
- How do we compare biometric entropy to password entropy?
 - Direct equality e.g. FAR = PW raw entropy?
 - Makes no allowance for different potential for retries in the 2 cases
- Need to equate real rather than raw entropies

Password/Biometric Comparison

Illustrative Example

- Password – 4 Digit PIN
 - Raw entropy 10000
 - Real entropy ~5000 (see CC V2 CEM Annex B.8.3)
 - Assume 100 retries (over period of time)
 - Chance of success 1 in 50
 - **N.B. CC CEM V2 B.8.3 rates this as SOF Basic**
- Biometric – FAR 1%
 - Raw entropy 100
 - Real entropy = 100 / no of attempts possible
 - Same order of magnitude as 4 digit PIN example

Common Criteria - Common Methodology for Information Technology Security Evaluation

Biometric Evaluation Methodology Supplement [BEM]

Table 11: SOF defined in Terms of FAR

Strength of Function Level	Maximum FAR
SOF-Basic	0.01 (1 in 100)
SOF-Medium	0.0001 (1 in 10,000)
SOF-High	0.000001 (1 in 1,000,000)

In Summary

Pros and Cons of the Component Approach

- Accounts for all elements that contribute to security
- Provides a more realistic view of the actual security achieved
- Avoids undue emphasis on one element of the security picture

But -

- Demands reappraisal of established security paradigms
- Hard to quantify procedural elements
- Difficult to develop / agree comparable scaling of axes.
- Results may conflict with previous cultural “wisdom”

Work in progress

Current UK Government Thinking on Authentication Policy

Developed by Brian Holman
CESG ID&A Policy Developer
brian.holman@cesg.gsi.gov.uk

© Crown Copyright. All rights reserved.

The Password / Biometric Trade-off

Government Health Warning

This approach has been developed for internal Government Users (employees).

It was not developed with citizen-Government authentication in mind, but the approach may be useful for future e-government authentication

CAUTION

How should we combine Passwords and Biometrics?

Approach based on existing UK Government Risk Assessment Methodology –

HMG InfoSec Standard 1 (IS1)

Risk Assessment – IS1

Threats

no of attackers

type of attackers

opportunity

consequence of failure

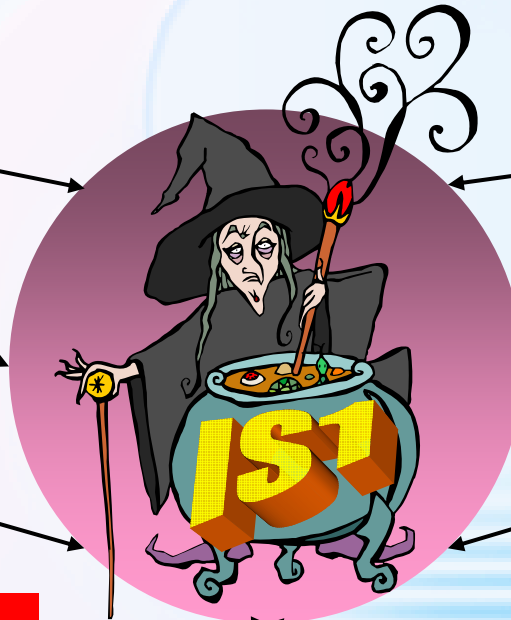
Mitigating Factors

environmental factors

technical factors

level of monitoring

available assurance



IS1 Password Length vs. Residual Risk

Typical Results

Residual Risk = 12 \Rightarrow 4 digit PIN

Residual Risk = 14.5 \Rightarrow 8 characters

Residual Risk = 17.5 \Rightarrow 12 characters

Overview of Steps

- Use IS1 to work out Residual Risk for given application
- Use existing policy advice to determine authentication password length requirement
- Use new policy advice to determine password length reduction allowed by introduction of biometric authentication.

New Policy - Trade off Password Length by adding Biometrics

- We invented a trade-off rule that simply “feels about right” – calibrated against hypothetical examples
- Like IS1 itself, it’s a pragmatic approach – don’t look too closely at the theory

Trading off Passwords and Biometrics

- Adding a biometric system reduces the Level of Residual Risk
- As we already have policy for assessing password length against Residual Risk, then we can use the same approach to translate reduction in Residual Risk into reduction in password length
- So the question resolves to: ***what is the reduction in Residual Risk provided by the biometric authentication?***

Trading off Passwords and Biometrics

- The Risk Level reduction “formula” used is based on a combination of:
 - The FAR of the biometric mechanism
 - A formal Common Criteria assurance measure
 - A Common Criteria Vulnerability Assessment level – the latter two to ensure there is no obvious weakness such as an easy bypass

Biometric Risk Level Reduction

Reduction in Risk Level	FAR	EAL	Vulnerability Assessment Level
5	1 in 10^5	5	AVA_VLA.3
4	1 in 10^4	4	AVA_VLA.2
3	1 in 10^3	3	AVA_VLA.2
2	1 in 10^2	2	AVA_VLA.1
1	1 in 10^2	1	None

© Crown Copyright. All rights reserved.

Trading off Passwords and Biometrics

Examples

- A good Biometric, i.e. a FAR better than 1 in 10^5 , assured to EAL5, will reduce a Password typically by 6 characters
- A poor biometric, i.e. FAR ~ 100 , assured to EAL1, will reduce a password by typically 1 character

But we never use less than a 4-digit PIN

Trading off Passwords and Biometrics

We don't consider the False Rejection Rate

That's up to each department or agency to decide what is or is not acceptable

“We’ve replaced one very high but rickety wall with a lower less rickety wall and a moat”

Brian Holman

**Thank you for your
attention**



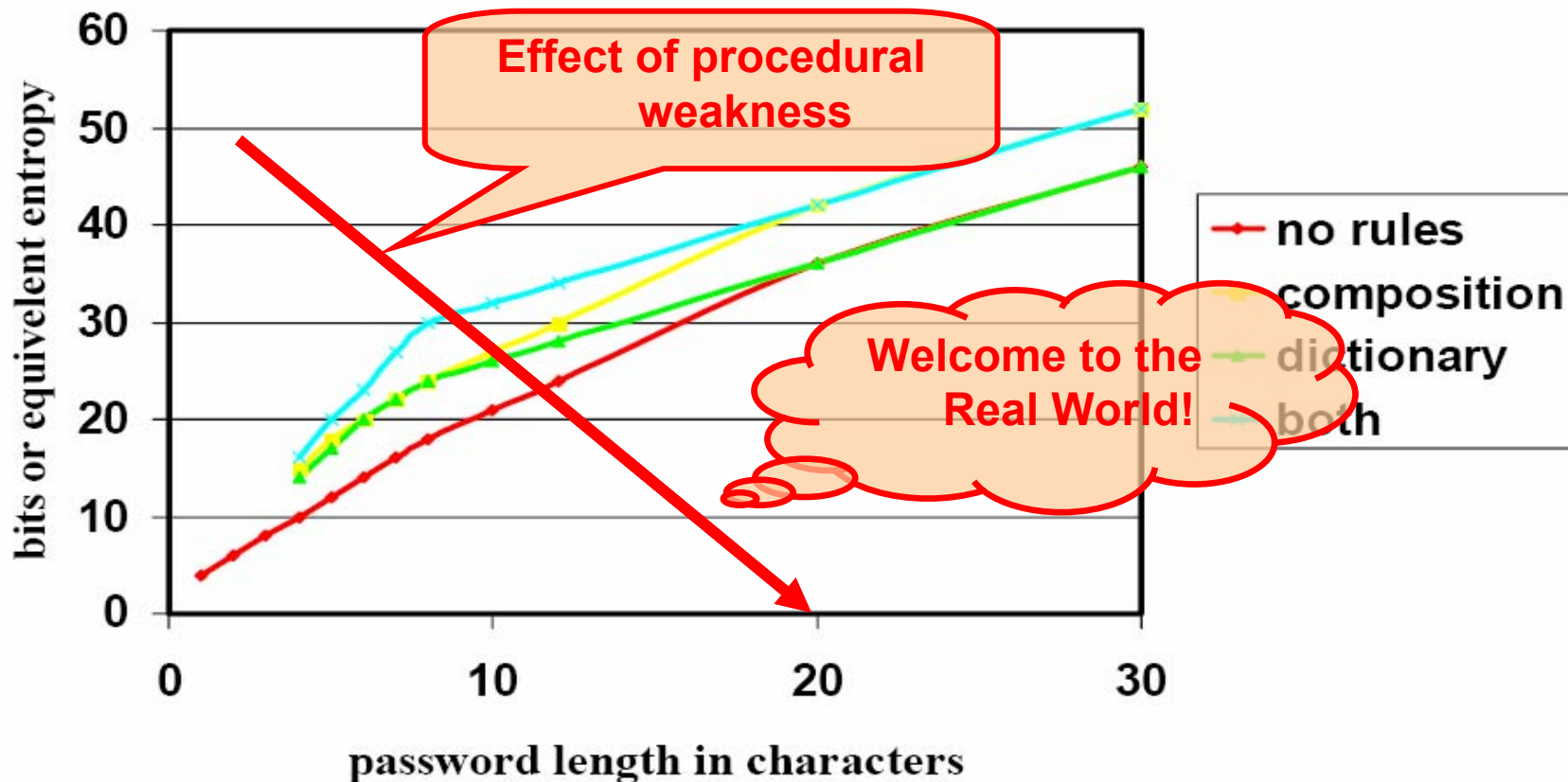
Further Information

www.cesg.gov.uk

– click on biometrics link

Questions?

Very Rough Password Entropy Estimate



Bill Burr: william.burr@nist.gov

NIST Knowledge Based Authentication Symposium Feb. 9, 2004