

Tales of Multimedia Security

Larry O’Gorman

*Avaya Labs Research
Basking Ridge, NJ, USA
logorman@avaya.com*

What is Multimedia Security?

Multimedia Security involves the combination of:

- Signals – speech, audio, image, web, video, VoIP
- Security – cryptography, system security, cryptanalysis

Multimedia Security often involves the fields of:

- Signal/image/video processing, and/or
- Cryptography

And sometimes involves standards:

- Security: AES, 3DES, RSA, DSA, SHA
- Signal: MPEG, JPEG

Keywords:

digital rights management, watermarking, steganography, biometrics, fingerprinting and traitor tracing, perceptual hashing, joint signal processing and encryption, signal processing in the encrypted domain, biometrics, digital forensics

Outline

Multimedia Security Projects:

- (~1992) Watermarking for *RightPages*® Digital Library
- (~1995) Counterfeit-resistant ID card, *PositiveID*
- (~1999) Fingerprint anti-spoof
- (~2000) Fingerprint “swipe” capture
- (~2002) VoIP security for distributed network monitoring
- (~2003) SPIT – SPAM over Internet Telephony
- (~2003) Avaya *Viper* VXML-based password reset system
- (~2005) Spoken Password (*SPIN*) for wireless authentication
- (current) (Speech Analytics – although uses speaker verification techniques, is not for security application)

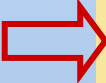
Bell
Labs

Veridicom

Avaya
Labs

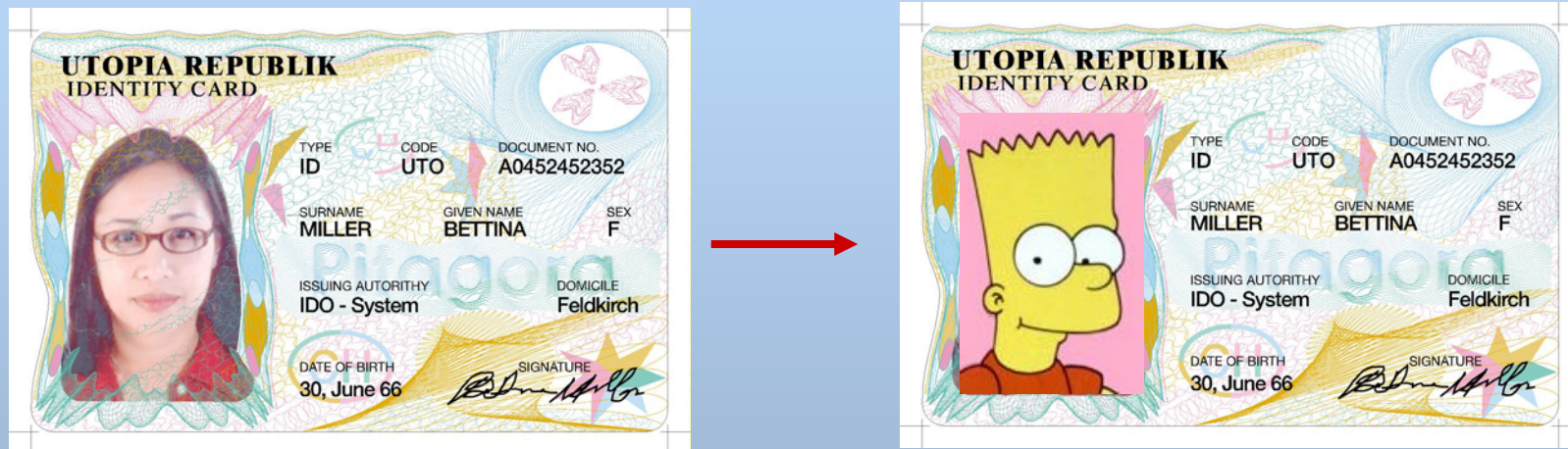
Outline

Multimedia Security Projects:

- 
1. Counterfeit-resistant ID card, *PositiveID*
 2. Fingerprint anti-spoof and “swipe” capture
 3. Spoken Password (*SPIN*) for wireless authentication

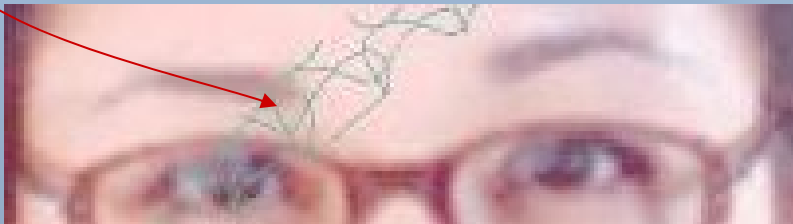
Counterfeit-Resistant ID Card

The most common form of counterfeit ID card is a legitimate card whose photo has been changed to that of an imposter.



Counterfeit-Resistant ID Card

Current card technology contains safeguards against such counterfeiting, but this requires a human “gatekeeper”.



ID cards are commonly protected with various chemical, printing, and optical means – in this case intaglio overprinting on the photograph, which is present on the legitimate ID, but absent on the counterfeit.

Counterfeit-Resistant ID Card

Positive ID Project

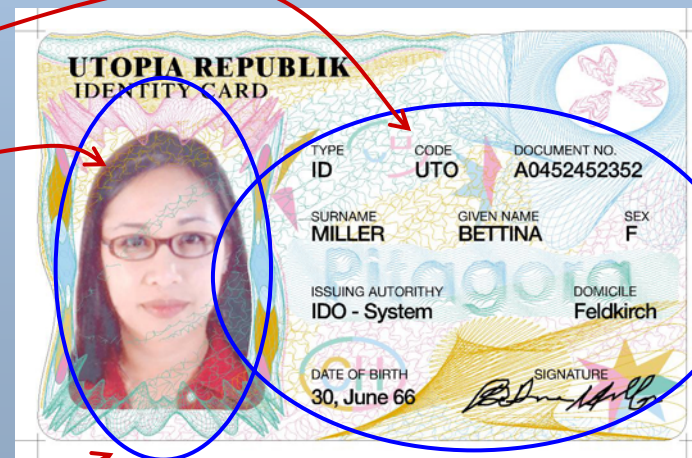
Objective

Design a card whose legitimacy could be determined by machine.

What does “legitimacy” mean?

For ID documents, it is tying the true textual information on the card to the true photograph on the card. So, although the card could be duplicated, its two bodies of information should be unchangeable and inextricable.

1. Cannot change text
2. Cannot change photo
3. Photo and text inextricable.



Counterfeit-Resistant ID Card

Two Components to the Positive ID Technology

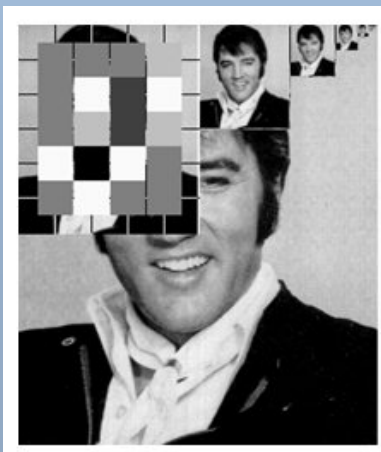
1. **Image Processing** – this involves some sort of “signature” of the photograph. We will call this the *image signature* to distinguish it from the *digital signature*.
2. **Security** – some way to tie photograph and text information together – this is where the *digital signature* is used.

Counterfeit-Resistant ID Card

Positive ID Technology – Image Processing

A signature is computed of the photograph that involves *multi-resolution processing* for 2 reasons:

1. A multi-resolution image representation involved overlapping areas on a single scale and overlapping information on different scale levels, so if one were to try to alter features, these would affect other features both spatially and scale-wise.
2. A multi-resolution representation efficiently represented all areas and scales of the image.



This example shows multiple resolutions of the same photograph. At each resolution level an array of values is extracted. These are just average values. These values make up the image signature. In this example,

Sig = {(4x5 level 1 values), (4x5 level 2 values), etc.}

Counterfeit-Resistant ID Card

Positive ID Technology – Image Processing

Cards were weathered over 2 seasons atop a roof at Bell Labs.

After this, their image signatures were extracted and matched to determine robustness of photo-signature algorithm.



Roof at Bell Labs, Murray Hill, NJ.
Card rack was here facing south.



Card rack containing weathering cards on a snowy day.

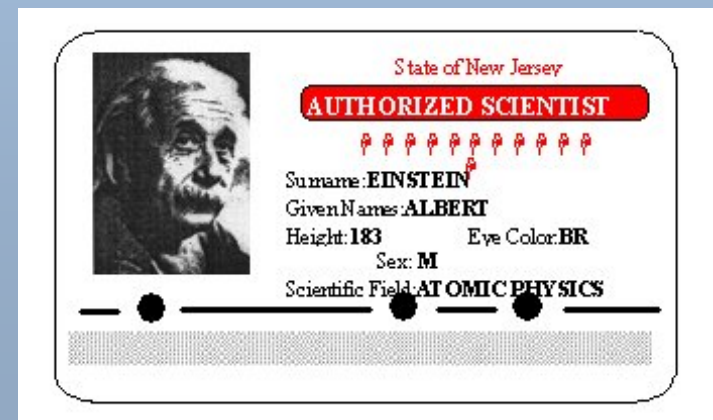
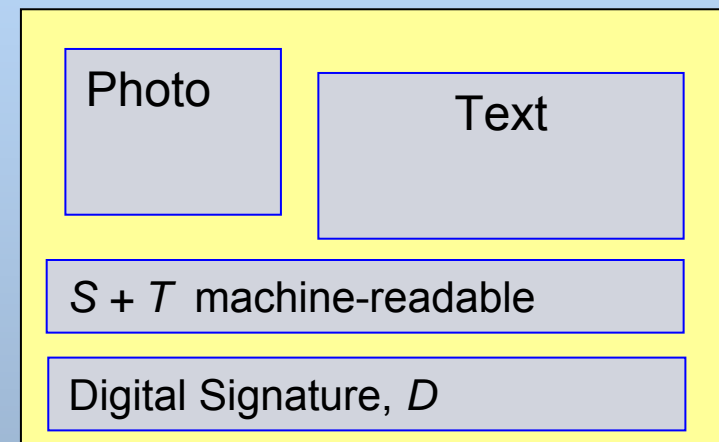
Counterfeit-Resistant ID Card

Positive ID Technology – Security

Public key cryptography is used for security in the following way:

1. Secure Card Creation

- a) Image Signature, S , is found from photo. This is a feature vector,
 $S = \{f1, f2, \dots\}$.
- b) S is printed on the card in *plaintext*.
- c) The text is already written on the card for human reading. It is also concatenated for machine reading,
 $T = \{\text{Einstein_Albert_183_BR} \dots\}$.
- d) Signature and text are concatenated,
 $T = S + T$, then hashed (1-way function),
 $h = H(S + T)$ (160-bit SHA-1 hash).
- e) Hash result is encrypted using private key,
 $D = E(h)$,
 and this digital signature is printed on the card.

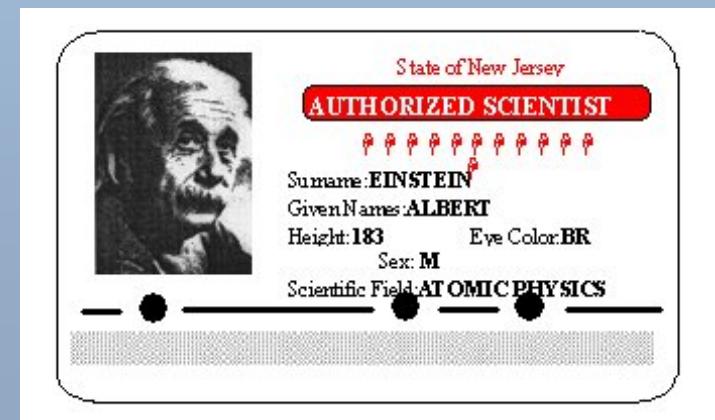
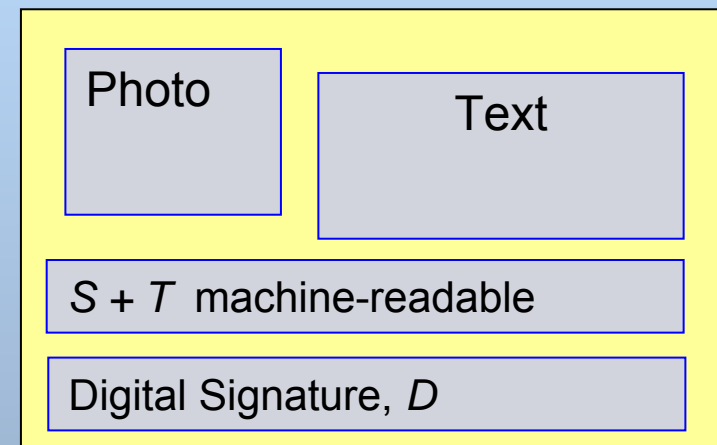


Counterfeit-Resistant ID Card

Positive ID Technology – Security (cont.)

2. Card Authentication

- a) Card is optically scanned and text and photo are separated for separate analyses.
- b) Text and image signature ($S + T$) are read from machine-readable area.
- c) Image signature is found from photograph, S' , and compared with one read from card, $S \approx S'$, allowing for inexact matching.
- d) Text and signature read from card are concatenated and hashed, $h' = H(S + T)$.
- e) Digital signature is read, decrypted using public key (of the private-public key pair), and compared against the hash, $h = ? h'$.
- f) If $S \approx S'$ and $h = h'$, then card (including photo and text) is legitimate.



Counterfeit-Resistant ID Card

Retrospective on Positive ID

1. A paper on this work won the Best Industrial Paper Award at Int. Conf. Pattern Recognition, ICPR '96 and an award for one of the best patents of the year at Bell Labs.
2. The technology was licensed from Lucent and a company started with it, AuthX.
3. The method has enjoyed success elsewhere.



Reference:

L. O’Gorman, I. Rabinovich, “Secure identification documents via pattern recognition and public-key cryptography,” IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 20, No. 10, Oct. 1998, pp. 1097-1102.

Outline

Multimedia Security Projects:

1. Counterfeit-resistant ID card, *PositiveID*
- ➔ 2. Fingerprint anti-spoof and “swipe” capture
3. Spoken Password (*SPIN*) for wireless authentication

Fingerprint Biometrics



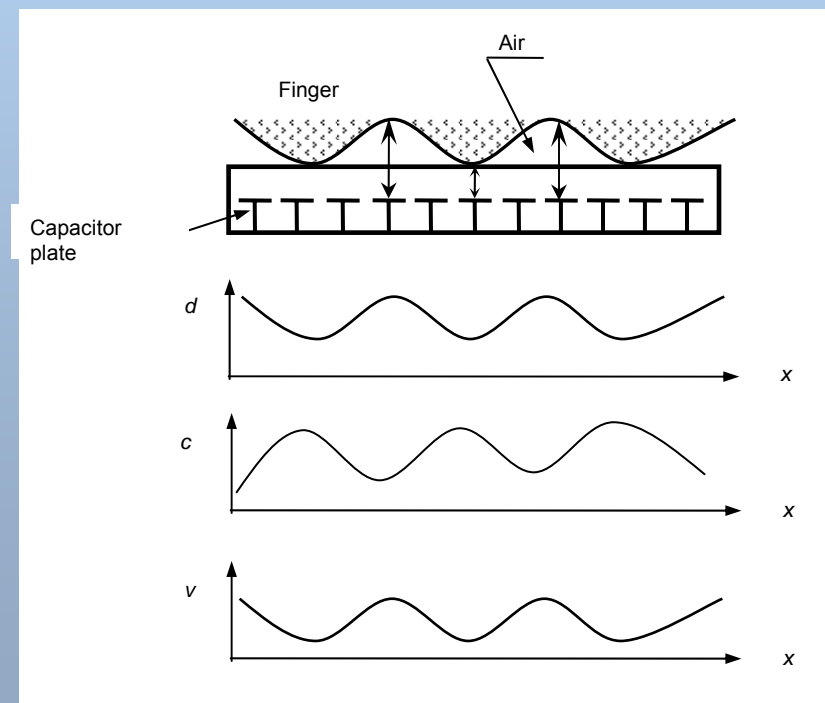
Background – Solid-State Fingerprint Sensor:

The capacitive sensor evolved from CMOS camera design in the 1990s. Basically, the photo-sensor array was replaced by an array of capacitors. The array is typically 250x300=75,000 pixels and the capacitors are small, typically 50um, so the entire array comprises the size of a fingerprint. The capacitors must be smaller than the width of the ridges and valleys to resolve these features.

Capacitors have two plates, one plate is built within the sensor, and the other plate is considered to be the skin of the fingerprint. Capacitance varies as a function of the distance between the plates, so the fingerprint ridges and valleys can be differentiated on the basis of their capacitive measurement,

$$C = k * (s / d)$$

Where **C** is the capacitance, **k** is the dielectric constant, **s** is the surface area of the capacitor, and **d** is the distance between the electrodes of capacitor.



Fingerprint Biometrics

Fingerprint Anti-Spoofing:

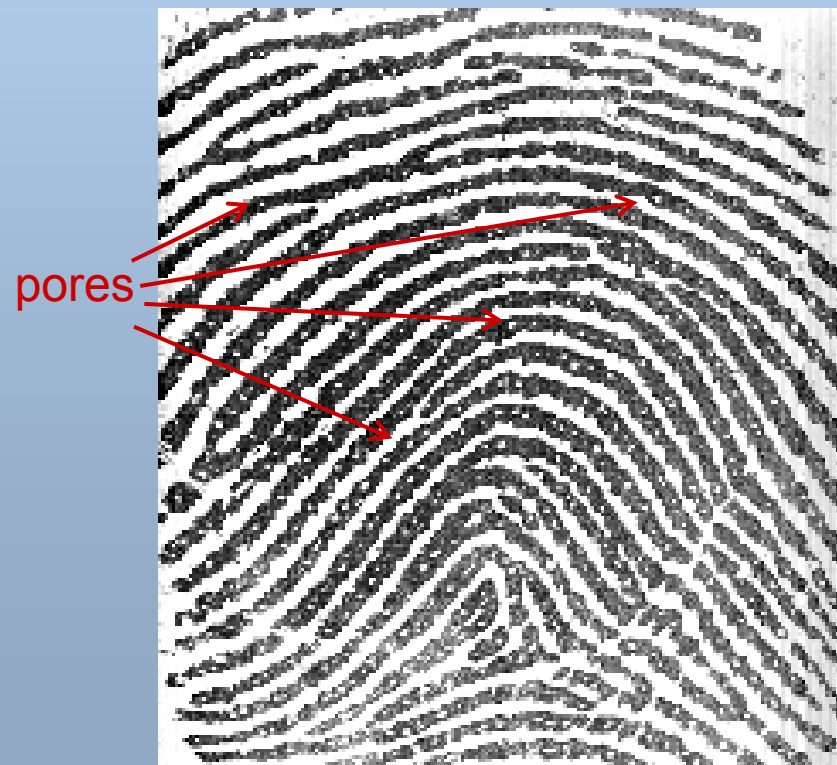
“Fingerprints are the ultimate secure identifier: you can’t forget them, no one can steal them, and they are unique.” (Sales pitch for the emerging commercial biometrics market)

Unfortunately, none of these statements is exactly correct.

We teamed with scientists at West Virginia University to design a “skin vitality” test that capitalizes upon two factors:

1. New gains in resolution of solid-state capture devices that enabled capture of skin pores.
2. Dynamic properties of living skin tissue.

Basically, living skin tissue sweats, so a dynamic sequence of fingerprints are captured and sweat activity examined around pores.



Fingerprint Biometrics

Retrospective on Fingerprint Work

1. There has been more realization since the halcyon early days of commercial biometrics (1990s) that biometrics is not a “silver bullet”.
2. Once out of the company, I was able to more objectively assess the security of biometrics. I compared biometrics with other authenticators in a paper*, and I formulated a challenge to biometrics scientists and vendors, what I called the,

Paradox of Secure Biometrics:

- i. A biometric is unique. So, it's secure.
- ii. But, unique means we can't change it if compromised. So, that's not secure.
- iii. And a biometric is not secret, so it can be easily compromised. That's *very* insecure.
- iv. So, is a biometric really secure?

References:

- *L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040.
- R. Derakhshani, S. Schuckers, L. Hornak, L. O'Gorman, "Determination of Vitality from A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners," Pattern Recognition, Vol. 36, No. 2, Feb. 2003, pp. 383-396.

Outline

Multimedia Security Projects:

1. Counterfeit-resistant ID card, *PositiveID*
2. Fingerprint anti-spoof and “swipe” capture
- 3. Spoken Password (*SPIN*) for wireless authentication

How to Securely Speak an Authentication Secret

MACCS Deployment at Johns Hopkins Medical Center

- Johns Hopkins Children's Center
- Installed in a particular surgical unit, which is a working unit, but is also designed for experimenting on the future of patient care

Wireless headsets

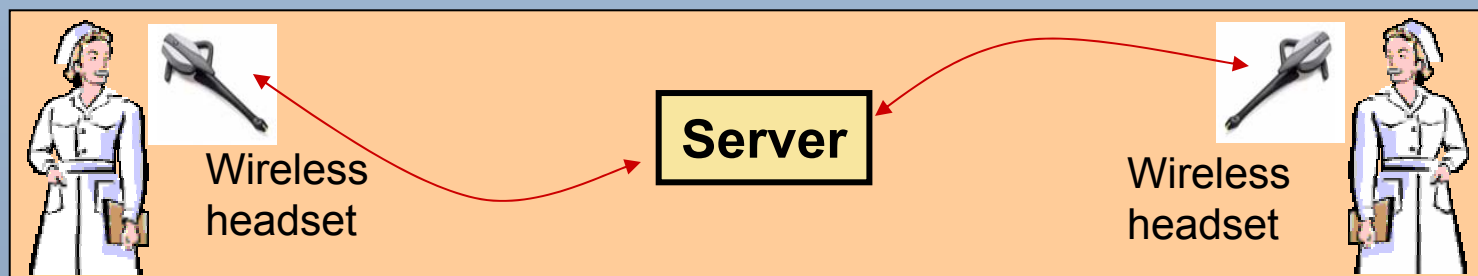


How to Securely Speak an Authentication Secret

Background

MACCS Project (Mobile Access for Converged Communications)

- Communications system for mobile workers whose job often requires exclusive use of their hands
- E.g., electronics clean room workers, health care workers, retail clerks
- Mobile, wireless headset (Bluetooth or IEEE 802.11)
- Spoken commands (no keyboard or keypad)
- “Presence” is known, i.e., location of active users
- Users can interact with system or with each other
- Prototype deployment at Johns Hopkins Medical Center

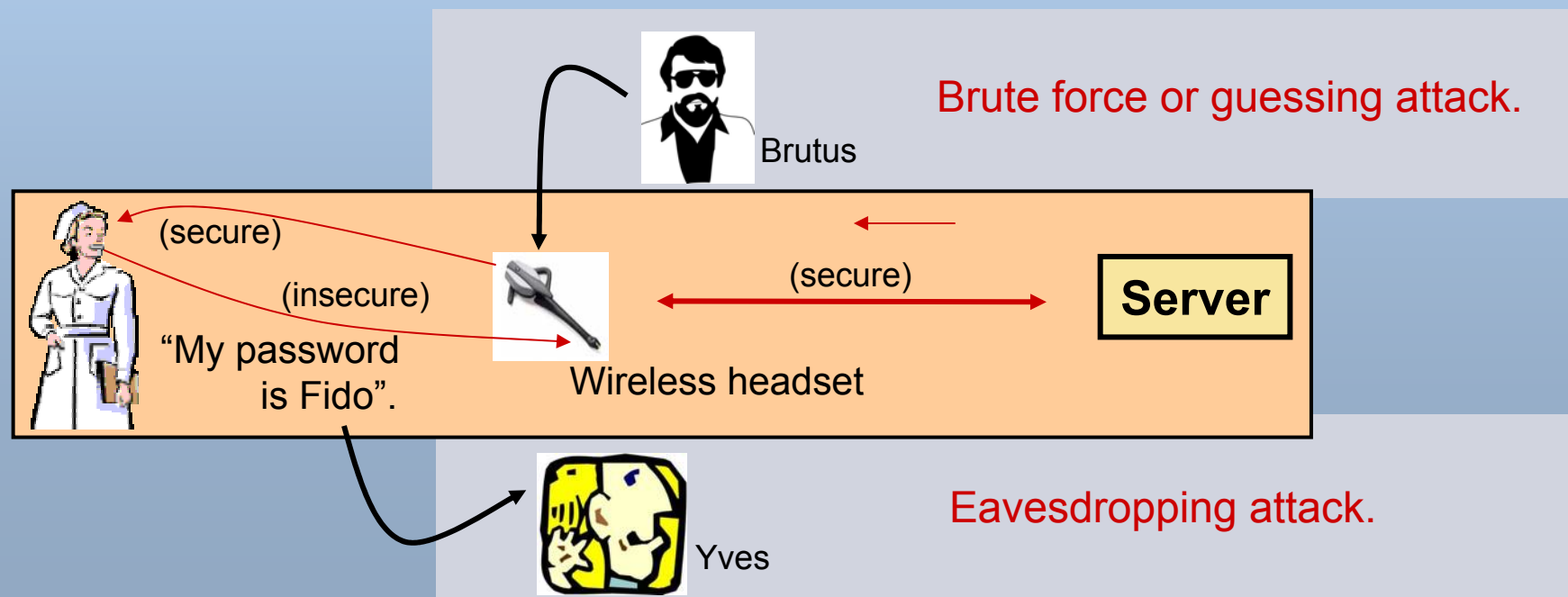


How to Securely Speak an Authentication Secret

MACCS Security Requirement – For privacy and security reasons, required to authenticate headsets to users. So, we have to authenticate headsets.

Main Threat Assumptions:

1. Attacker can hear voiced authentication response. (Yves, eavesdropper)
2. Attacker can hear and respond to challenges. (Brutus, brute force attacker)
3. Attacker **CANNOT hear challenge AND corresponding user responses.**



How to Securely Speak an Authentication Secret

Potential Solutions:

1. **Speaker Verification** would be wonderful if it were reliable.
SV error rates about 1-10%, much more for noisy areas, like hospitals.
2. **Yes/No Answers** from randomly ordered questions.
E.g., “Do you dye your hair?” y/n, “Do you eat beets?” y/n, ...
3. **Multiple Choice Q&A**, randomly ordered.
E.g., “What was the color of the car on which you learned to drive?
1) red, 2) blue, 3) green, 4) black, etc.”

Solution 3 was used initially and then offered as an option for MACCS. We call this procedure **QDP (Query-Directed Passwords)**.

QDP requires low memory effort of user, but takes some time to get through questions (for a specified security strength), about 15 seconds per question or 1.5 minutes for full session as used for this application.

→ QDP takes too long to authenticate. Is there a quicker procedure?

How to Securely Speak an Authentication Secret

Approach and Definitions:

1. **Challenge-Response** – response changes each authentication, so eavesdropper cannot just repeat it

2. **Substitution Cipher** –

e.g., **Substitution rules: Red → 3, Green → 2, Blue → 9, Yellow → 6**

Challenge: “Blue, Red, Yellow, Green”

Response: “ 9, 3, 6, 2”

But, eavesdropper will very quickly learn there are only 4 code elements, resulting in only $4! = 24$ permutations, so randomly insert *camouflage elements*.

3. **Camouflage Elements** –

e.g., **Challenge: “1, 8, Blue, 4, Red, Yellow, 0, 7, Green, 5”**

Response: “1, 8, 9, 4, 3, 6, 0, 7, 2, 5”

Now the number of permutations is $10 \times 9 \times 8 \times 7 = 5040$.

4. **Security** – security strength is measured as the number of total guesses a brute force attacker would have to make to be assured of obtaining the correct response – in this paper, it’s related to the **permutations**.

How to Securely Speak an Authentication Secret

Method Evolution

Method a –Challenge-response on randomly ordered substitution elements

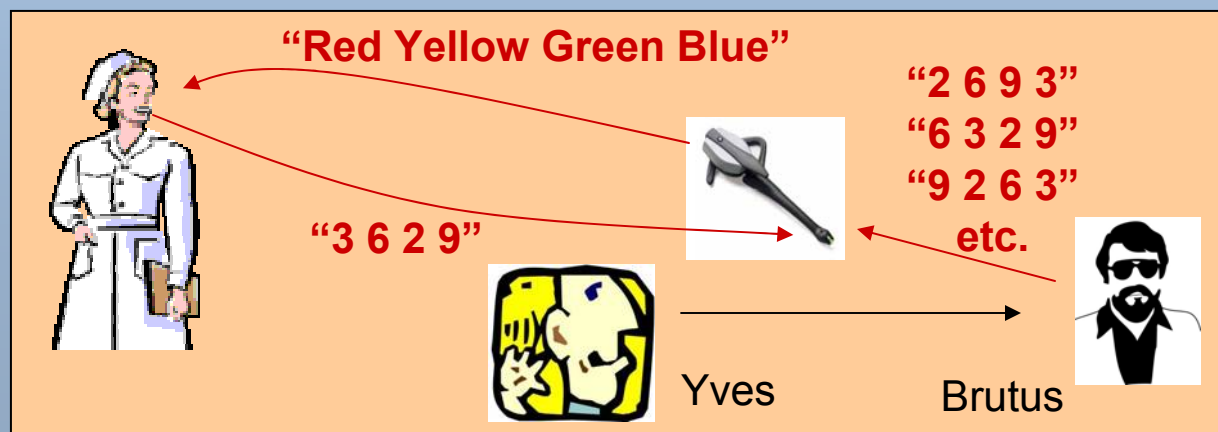
E.g.: Memorize color-number pairs: Blue=9, Red=3, Yellow=6, Green=2

Challenge: “Red Yellow Green Blue”

Response: “ 3 6 2 9”

Security: $L(L-1)\dots(L-k) = 10 \times 9 \times 8 \times 7 \rightarrow 4 \times 3 \times 2 \times 1$ after vulnerability

Vulnerability: Yves can learn digits and give to Brutus who tries few permutations



How to Securely Speak an Authentication Secret

Method Evolution (cont.)

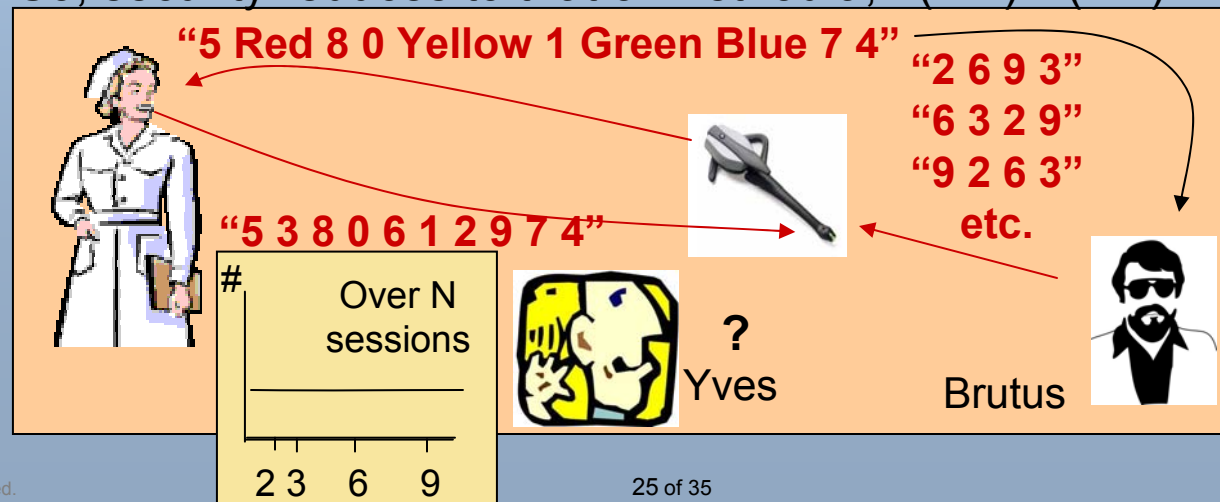
Method b – Method a, but add camouflage elements that are from the subset exclusive of authentication elements to obtain a uniform distribution of all elements, so they are chosen *dependent* on the authentication elements

E.g.: Challenge: “5 Red 8 0 Yellow 1 Green Blue 7 4”

Response: “5 3 8 0 6 1 2 9 7 4”

Security: $L(L-1)\dots(L-k) = 10 \times 9 \times 8 \times 7 \rightarrow 4 \times 3 \times 2 \times 1$ after vulnerability (same as a)

Vulnerability: Although Yves gains no information from challenges, Brutus can attack easily. He knows that colors correspond to all the numbers he does not hear. So, for above, he knows the colors are numbers {3, 6, 2, 9}. So, security reduces to that of Method a, $L(L-1)\dots(L-k) = 4 \times 3 \times 2 = 24$



How to Securely Speak an Authentication Secret

Method Evolution (cont.)

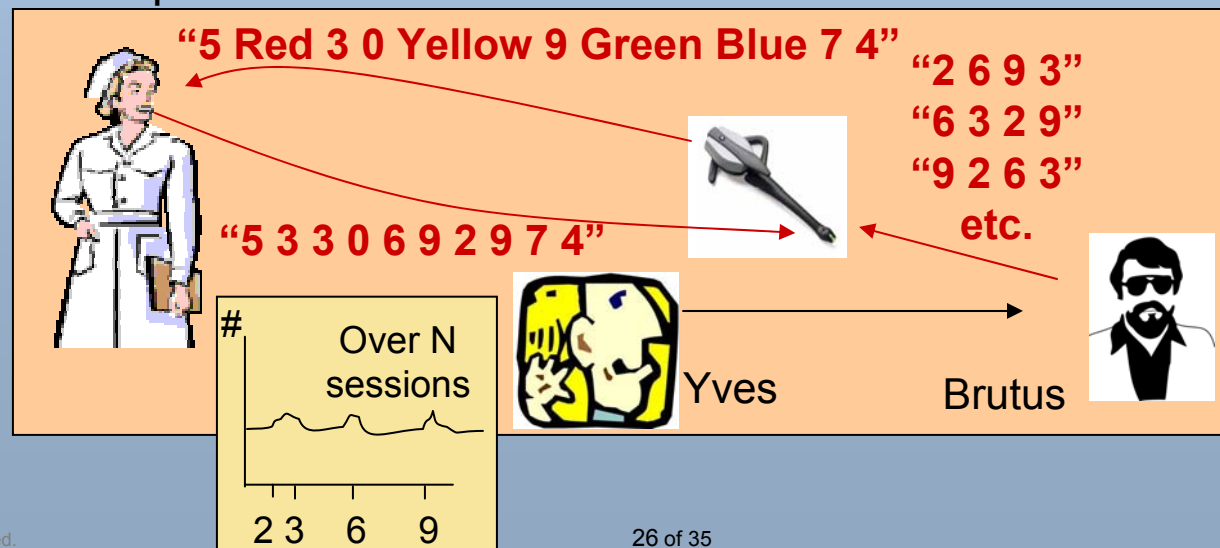
Method c – Method b, but add camouflage elements that are *independent* of authentication elements

E.g.: Challenge: “5 Red 3 0 Yellow 9 Green Blue 7 4”

Response: “5 **3** **3** 0 6 **9** 2 **9** 7 4”

Security: $L(L-1)\dots(L-k) = 10 \times 9 \times 8 \times 7 \rightarrow 4 \times 3 \times 2 \times 1$ (+ N sessions) after vulnerability

Vulnerability: Yves makes histogram over N sessions of responses, finds that authentication elements have higher frequency, gives elements to Brutus who tries permutations



How to Securely Speak an Authentication Secret

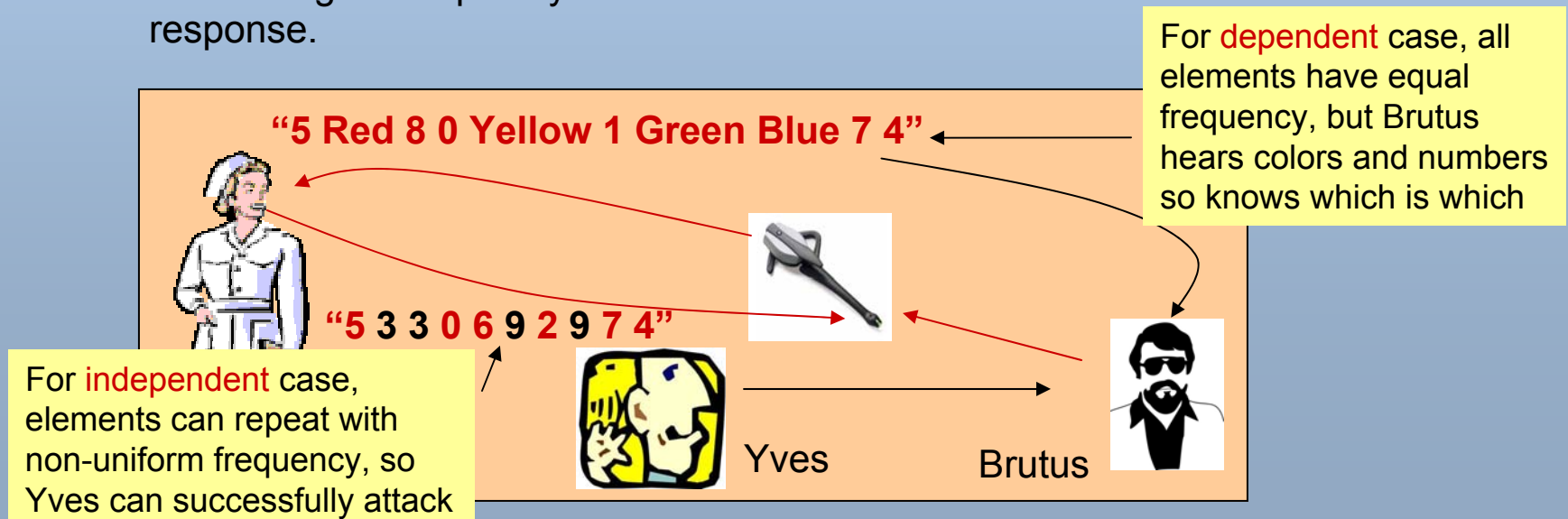
Method Evolution – Assess Situation to this Point

Case 1 – Dependent

If camouflage and authentication elements are **dependent** on each other so that they are uniformly distributed, then Yves gains no information from response. But Brutus can easily determine authentication elements from the challenge.

Case 2 – Independent

If camouflage and authentication elements are **independent** of each other then Brutus gains less information than from Case 1. But Yves can gain frequency information of authentication elements from the response.

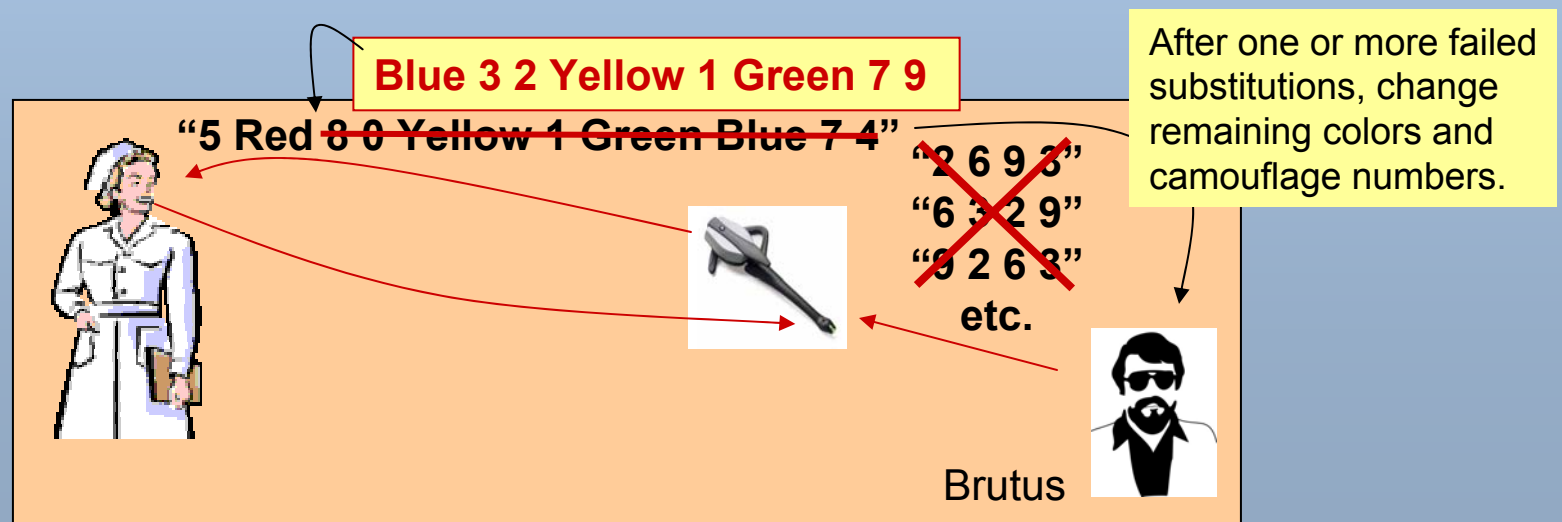


How to Securely Speak an Authentication Secret

But we haven't taken advantage of all we can ...

While we can't limit Yves' ability to eavesdrop, we can limit Brutus' attempts to guess:

1. After x erroneous authentication substitutions, mount counter-defense by "removing information" from rest of sequence.
2. After y erroneous authentication elements, freeze account.
3. We can also insert *independent* camouflage elements to the challenge (Method c), as long as the *dependent* camouflage elements are already there (Method b) to defend against Brutus.



How to Securely Speak an Authentication Secret

Method Evolution (cont.)

Method d –

i) Start with random order of authentication elements, e.g.,

“Red Yellow Green Blue”

(where Blue=9, Red=3, Yellow=6, Green=2)

ii) Randomly insert *dependent* camouflage elements (chosen to obtain uniform distribution)

“5 Red 8 0 Yellow 1 Green Blue 7 4”

ii) Randomly insert *independent* camouflage elements (chosen to reduce probability of Brutus knowing authentication elements from challenge)

“5 6 Red 8 1 6 0 Yellow 1 Green 4 Blue 7 4 9” (challenge)

“5 6 3 8 1 6 0 6 1 2 4 9 7 4 9” (response)



How many of each type of camouflage elements do we have to add?

How to Securely Speak an Authentication Secret

Security – Best Case, Worst Case (without c_i elements)

Best case is when all authentication elements occur at the beginning of the sequence:

e.g., “Red Green Blue Yellow 5 3 0 9 7 4” (with only c_D , no c_i elements)

In this case, Brutus must guess color substitutions without any information that can be gathered from knowing the camouflage elements.

Security strength is $L(L-1)\dots(L-m+1) = 10 \times 9 \times 8 \times 7 = 5040$

Worst case is when all authentication elements occur at the end of the sequence:

e.g., “5 3 0 9 7 4 Red Green Blue Yellow ” (with only c_D , no c_i elements)

In this case, Brutus has all the information on what values the colors are not equal to from the preceding camouflage elements.

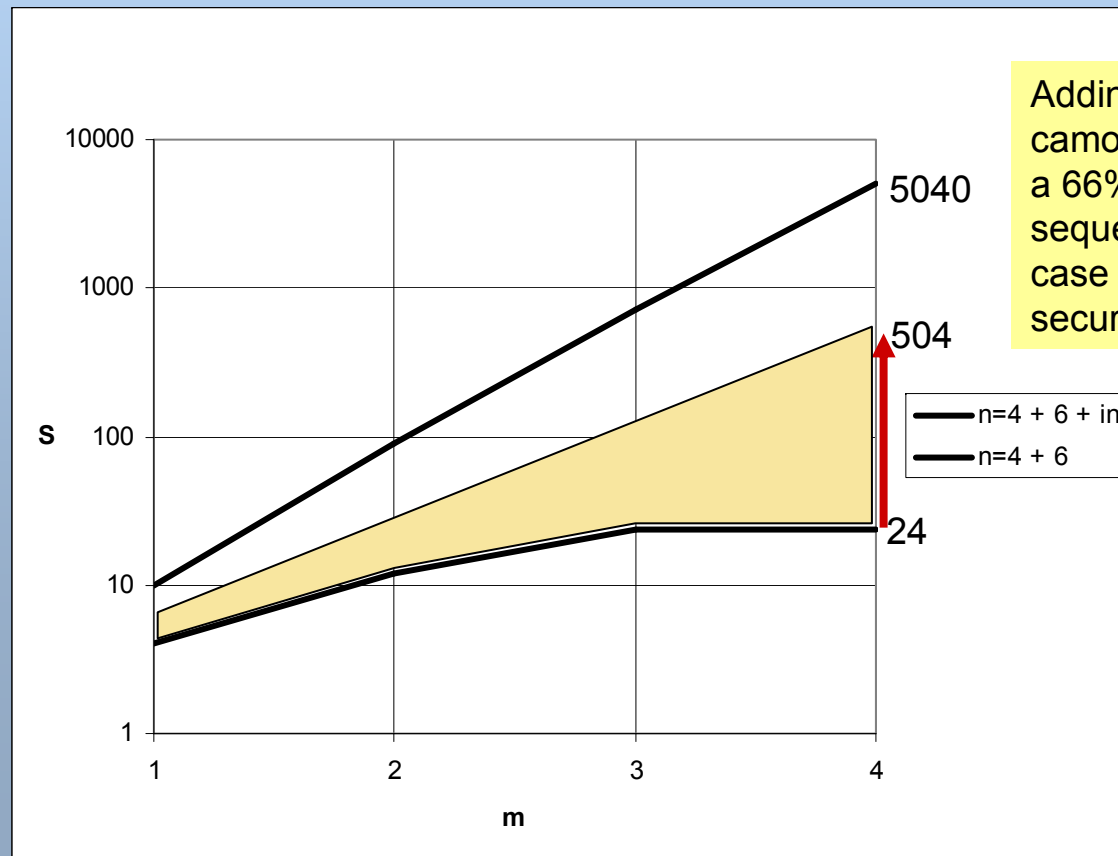
Security strength is $m! = 4! = 24$

How to Securely Speak an Authentication Secret

Security – Best-Case, Worst-Case (with c_i elements)

What number of inserted c_i elements will it take to improve worst case security strength from $m!$ to $(L-1)(L-2)\dots(L-m+1)$ with given probability?

e.g., $m=4$, $c_d=6$, $L=10$, $P = 66\% \rightarrow c_i=10$ gives $S = 9 \times 8 \times 7 = 504$



Adding $c_i=10$ extra camouflage elements gives a 66% likelihood that a sequence will have worst-case equivalent to $L-1$ security strength.

How to Securely Speak an Authentication Secret

SPIN Tradeoffs –

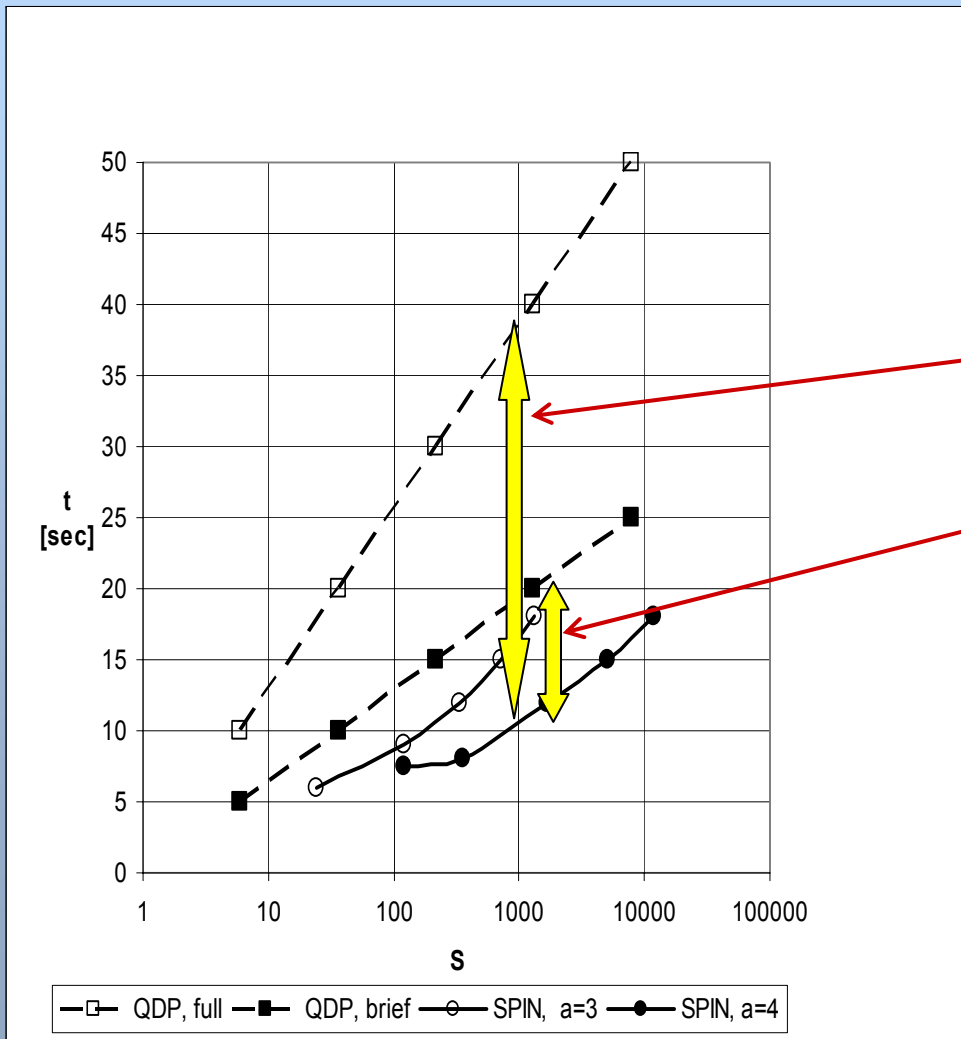
So, for the example we've been following:

- User has to memorize $m=4$ color-number pairs, $L=10$
- Minimum authentication length = 10 → min. security, $S=24$
- To achieve 66% probability of worst-case $L-1$ security strength or better, require an extra 10 elements,
- So, use $n=20$ to obtain security strength that ranges from $S=5040$ to $S=504$ with 66% probability on lower end.

A 20-length SPIN code takes about 20 seconds, so this is about 6x faster than the 1.5 minutes for QDP. What do users think? ...

How to Securely Speak an Authentication Secret

Comparing Memorized SPIN Versus “Remembered” QDP



Performed 2 Comparative Trials:

- Johns Hopkins Unit (35 users, 60 days)
- Avaya Labs (20 users, 2 weeks)

Results:

1. QDP(full) takes 4x longer than SPIN(4) for same security strength (40 seconds versus 10 seconds).
2. QDP(fast) takes 2x longer than SPIN(4) for same security strength (20 seconds versus 10 seconds).
3. Most users did not like 40 seconds for QDP(full).
4. Most users **VEHEMENTLY OPPOSED** memorizing for SPIN.
5. QDP(fast) was compromise, 2x slower than SPIN, but without memorization. This was preferred.

How to Securely Speak an Authentication Secret

Retrospective on SPIN and MACCS

1. The MACCS project may be developed into a communications product for the health-care market.
2. Although both SPIN and QDP(fast) spoken authentication methods will be offered, it's not clear which (if either) will win.



Reference:

L. O'Gorman, L. Brotman, M. Sammon, "How to speak an authentication secret securely from an eavesdropper," 14th Int. Workshop on Security Protocols, Cambridge, England, March 2006.

Summary

Multimedia Security Projects – this talk has focused on the topics below in red:

- (~1992) Watermarking for *RightPages*® Digital Library
- (~1995) Counterfeit-resistant ID card, *PositiveID*
- (~1999) Fingerprint anti-spoof
- (~2000) Fingerprint “swipe” capture
- (~2002) VoIP security for distributed network monitoring
- (~2003) SPIT – SPAM over Internet Telephony
- (~2003) Avaya *Viper* VXML-based password reset system
- (~2005) Spoken Password (*SPIN*) for wireless authentication
- (current) (Speech Analytics – although uses speaker verification techniques, is not for security application)

Extra Slides

Watermarking for RightPages® Digital Library

The Digital Library:

In the early 1990s, even before the World-Wide Web, researchers around the world began to think about digital libraries.

This was a very exciting time because it involved a paradigm shift, making books, pictures, and other media available electronically.

There were many technical challenges:

- Document image processing (at least for present and archival material)
- Hyperlink document models
- Formats (XML)

Three of the early libraries were:

- Vatican Library (IBM)
- US Patent Office (IBM)
- *RightPages* Service (AT&T Bell Labs)

Watermarking for RightPages® Digital Library

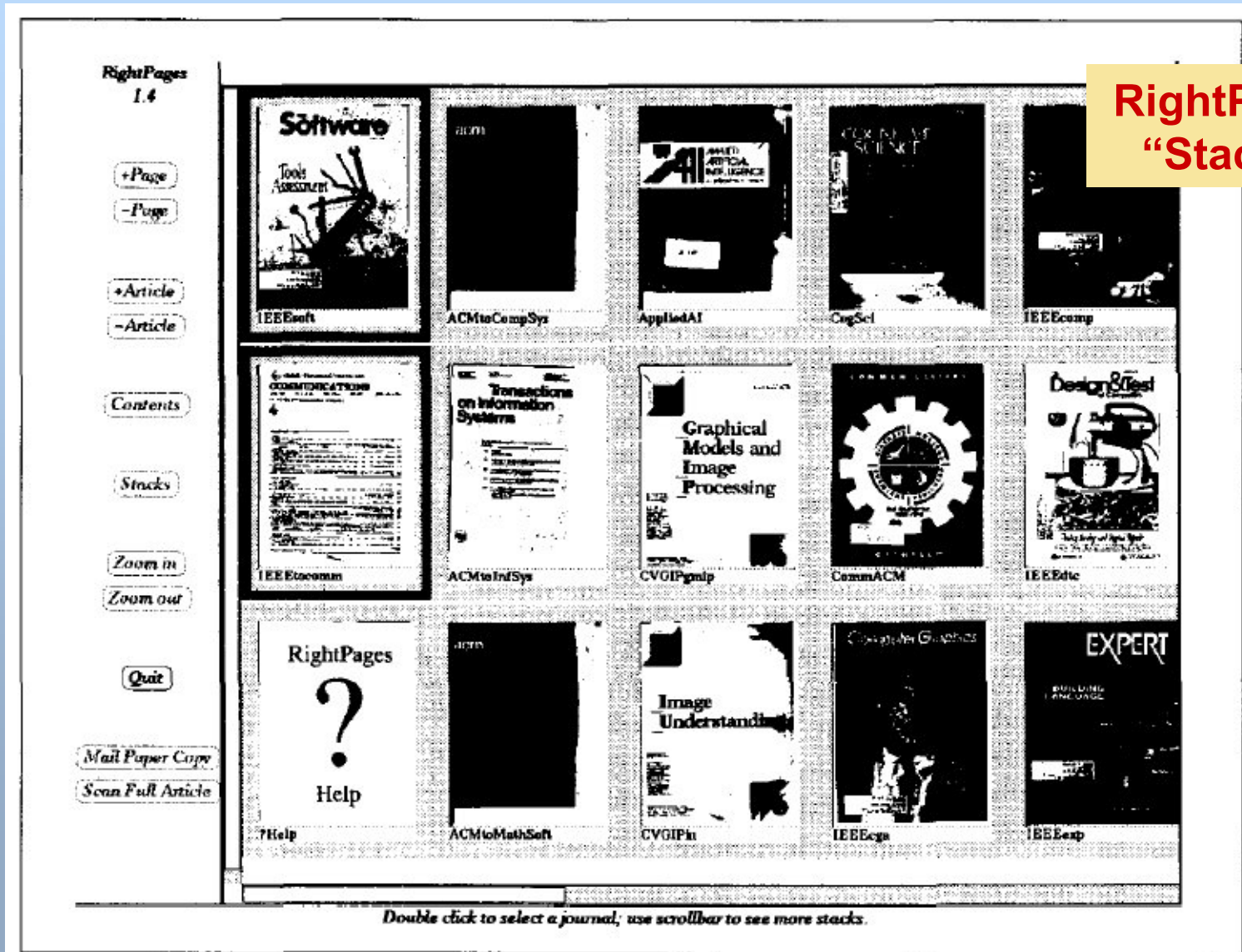
Bell Labs *RightPages* Digital Library:

RightPages was image-based (as indeed were most early libraries because pixels was the common standard between publishers).

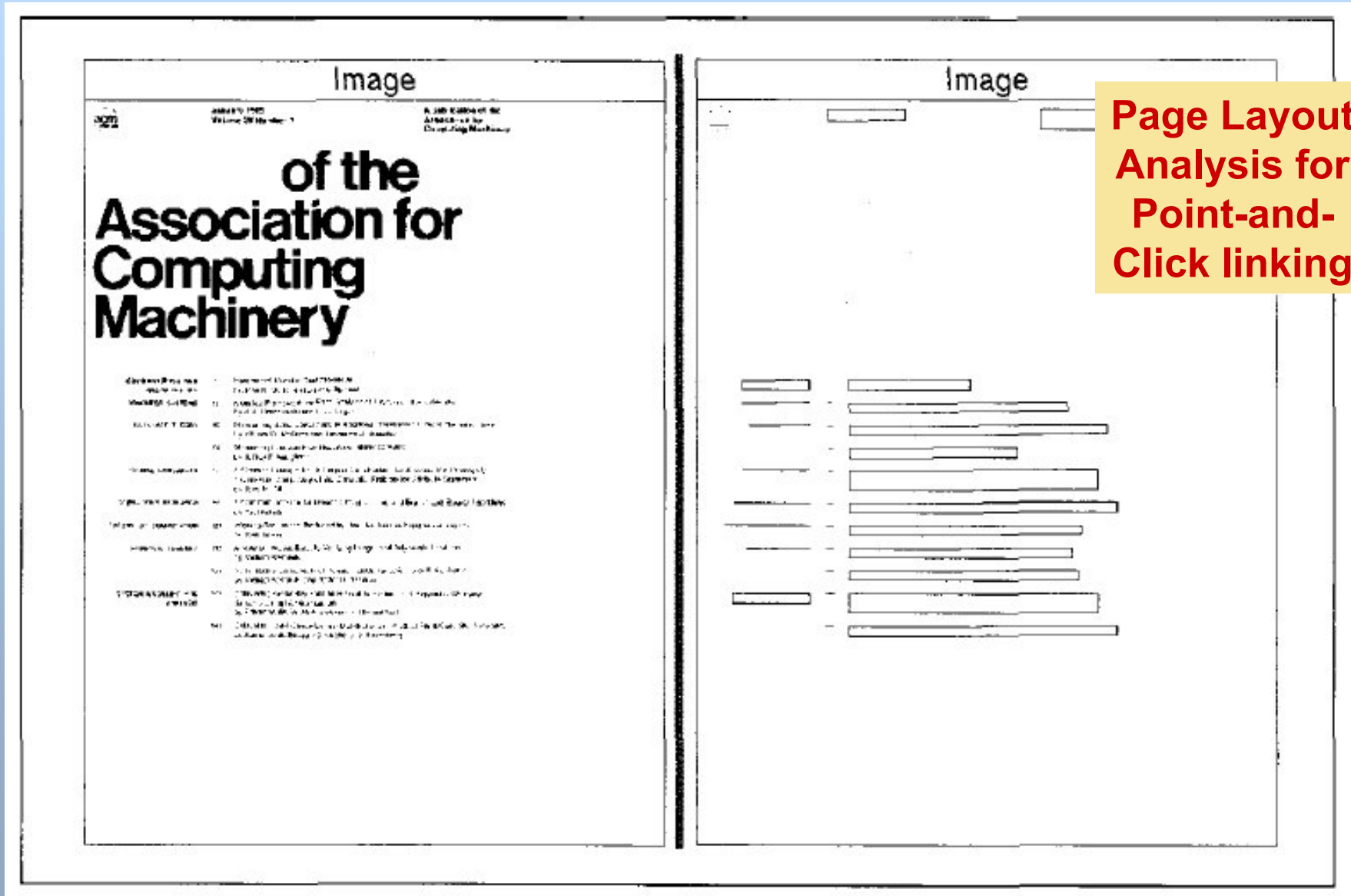
The technical perspective of RightPages was document image processing:

- Page scanning
- Picture/text segmentation
- Noise reduction
- Binarization
- Skew correction
- Page layout analysis
- OCR

Watermarking for RightPages® Digital Library



Watermarking for RightPages® Digital Library



Watermarking for RightPages® Digital Library

Bell Labs RightPages included:

Publishers : IEEE, ACM, Elsevier, Pergamon, American Institute of Physics, Academic Press, and others.

Journals : IEEE Spectrum; IEEE Computer; IEEE Expert; IEEE Software; IEEE Trans. Communications; IEEE Trans. Pattern Analysis and Machine Intelligence; IEEE Trans. Computers; IEEE Trans. Software; IEEE Selected Areas of Communications; IEEE Trans. Circuits and Systems; IEEE Trans. Software Engineering; Cognitive Science; Physics Today; Communications ACM; ACM Transactions on Information Systems; Journal of Algorithms; CVGIP Image Understanding; CVGIP Graphical Models and Image Processing; Artificial Intelligence; Computer Networks and ISDN Systems; Systems Integration; Acta; Pattern Recognition; Pattern Recognition Letters; Information Processing Letters, Systems Integration, and others

There were 2 other RightPages installations:

- **University of California at San Francisco Medical School**
- **Group of Pharmaceutical companies centered in NJ**

Watermarking for RightPages® Digital Library

Bell Labs RightPages included:

Publishers : IEEE, ACM, Elsevier, Pergamon, American Institute of Physics, Academic Press, and others.

Journals : IEEE Spectrum; IEEE Computer; IEEE Expert; IEEE Software; IEEE Trans. Communications; IEEE Trans. Fuzzy Systems and Machine Intelligence; IEEE Trans. Computers; IEEE Trans. Software; IEEE Selected Areas of Communications; IEEE Trans. Circuits and Systems; IEEE Trans. Software Engineering; Cognitive Science; Systems Today; Communications ACM; ACM Transactions on Information Systems; Journal of Algorithms; CVGIP Image Understanding; CVGIP Graphical Models and Image Processing; Artificial Intelligence; Computer Networks and ISDN Systems; Systems Integration; Acta; Pattern Recognition; Pattern Recognition Letters; Information Processing Letters, Systems Integration, and others

There were 2 other RightPages installations:

- **University of California at San Francisco Medical School**
- **Group of Pharmaceutical companies centered in NJ**

Watermarking for RightPages® Digital Library

Watermarking and Steganography:

Watermarking is the process of marking a document (or other media) for one of many purposes including showing ownership, attaching information, hiding information, etc.

Steganography is the process of hiding a message in media (subset of watermarking).



1. Gladney, Mintzer, Schiattarella, "Safeguarding Digital Library Contents and Users", D-Lib Magazine, 1997
2. Kahn, The Codebreakers, The Story of Secret Writing", Macmillan Publ., 1967

Watermarking for RightPages® Digital Library

3 Methods for Text Watermarking for RightPages:

1. Word-space watermarking for justified text (format operation)

the Internet aggregates traffic flows from many end systems. Understanding
the Internet aggregates traffic flows from many end systems. Understanding

2. Line-space watermarking (format operation)

the Internet aggregates traffic flows from many end systems. Understanding
effects of the packet train phenomena on router and IP switch behavior
will be essential to optimizing end-to-end efficiency. A range of interesting

1. Character Feature watermarking (pixel operation)

the impact it has on information providers and users. Over 100 speakers and 100
the impact it has on information providers and users. Over 100 speakers and 100
the impact it has on information providers and users. Over 100 speakers and 100

Watermarking for RightPages® Digital Library

One Watermark Metric is Information Capacity:

1. **Word-space watermarking for justified text (format operation)**

the Internet aggregates traffic flows from many end systems.
 the Internet aggregates traffic flows from many end systems.

Information Capacity =
 $\text{spaces/line} * \text{lines/page}$
 $\approx 10 * 60 = 600 \text{ bits/page}$
 $= 75 \text{ char} \approx 12 \text{ words}$

2. **Line-space watermarking (format operation)**

the Internet aggregates traffic flows from many end systems. U
 effects of the packet train phenomena on router and IP switch
 will be essential to optimizing end-to-end efficiency. A range

Information Capacity =
 $(\text{lines/col} - 2) * \text{col/page}$
 $\approx 58 * 4 = 232 \text{ bits/page}$
 $= 29 \text{ char} \approx 5 \text{ words}$

1. **Character Feature watermarking (pixel operation)**

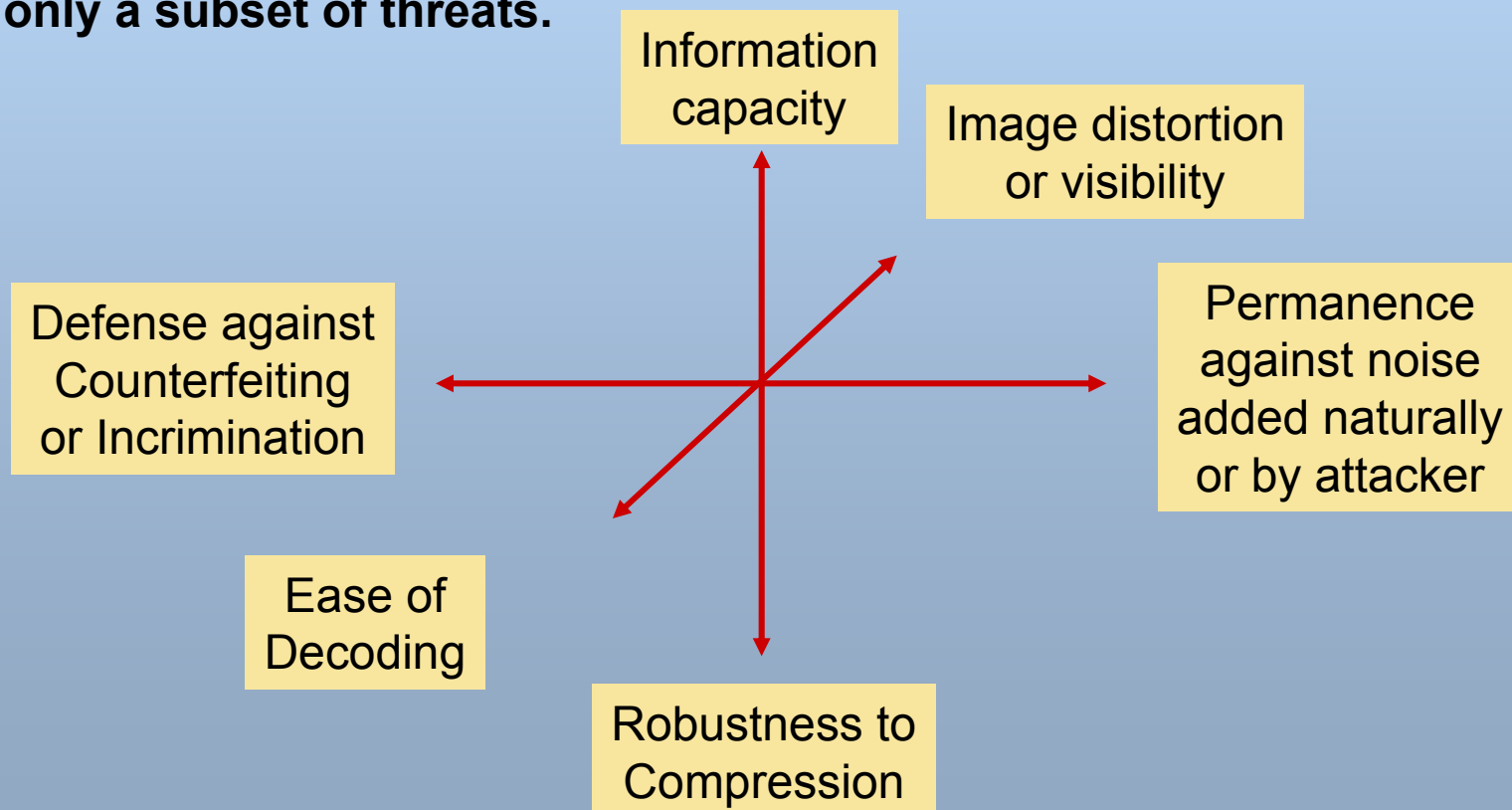
the impact it has on information providers and users. Over 100
 the impact it has on information providers and users. Over 100
 the impact it has on information providers and users. Over 100

Information Capacity is
 similar to method 1

Watermarking for RightPages® Digital Library

But watermarking has many parameter axes (depending upon the application). These trade off against one another.

A common failing in watermarking work that is used for security is to omit describing the **threat model**, then to design and test against only a subset of threats.



Watermarking for RightPages® Digital Library

Retrospective on RightPages watermarking

1. This work won an R&D 100 Award in 1996.
2. Breakup of AT&T and dispersal of researchers led to demise of RightPages.
3. Watermarking and digital rights management (DRM) are vital fields of work in the age of media content on the Web.



References:

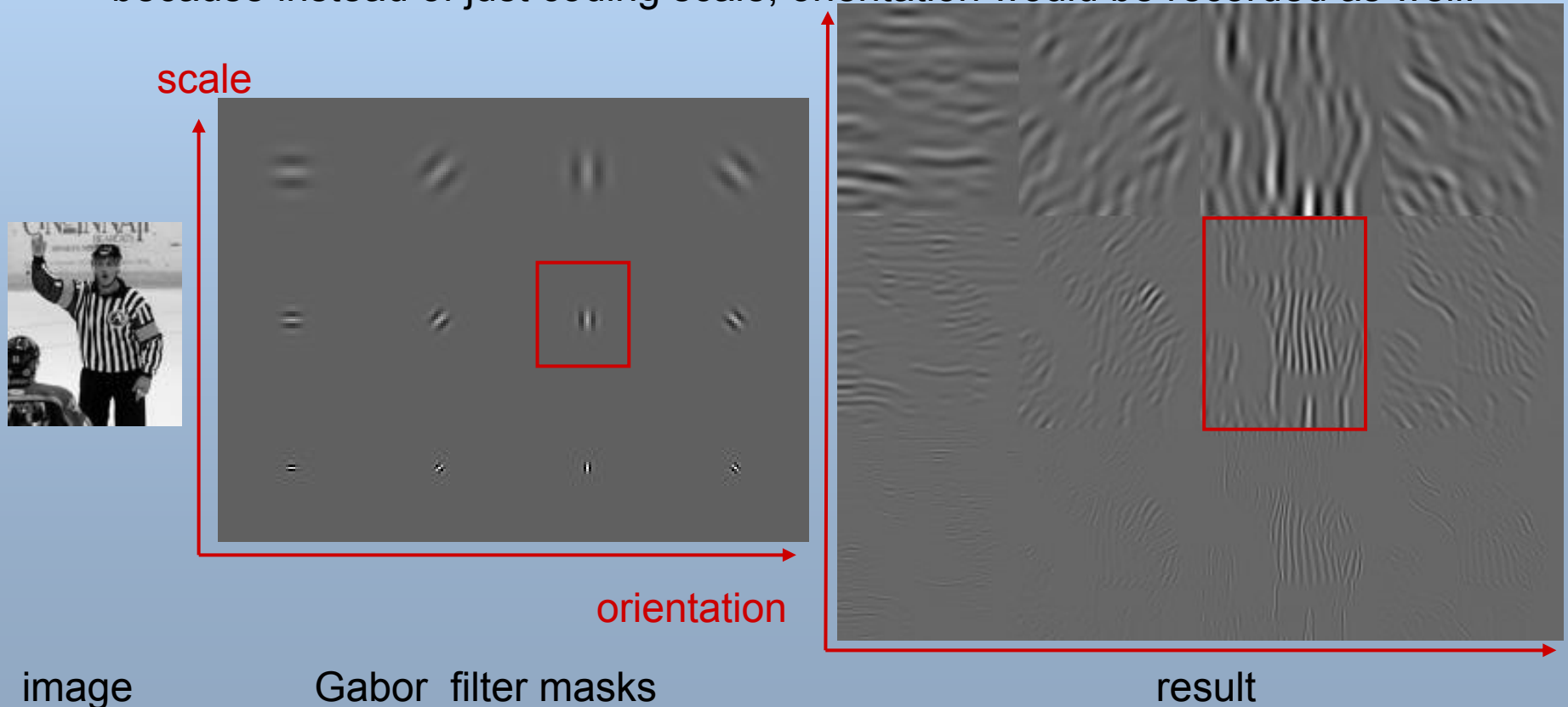
- J. Brassil, S. Low, N. Maxemchuk, L. O’Gorman, “Electronic Marking and Identification Techniques to Discourage Document Copying,” IEEE Journal on Selected Areas in Communications, Vol. 13, No. 8, Oct. 1995, pp. 1495-1504.
- L. O’Gorman, “Image and document processing techniques for the RightPages Electronic Library System”, Int. Conf. on Pattern Recognition (ICPR), The Hague, Sept. 1992, pp. 260-263.

Extra Slides

Counterfeit-Resistant ID Card

Positive ID Technology – Image Processing

In the mid-1990s at the time the Positive ID work was being done, wavelet functions were becoming popular for use in image processing, especially for coding. This would have been a more secure scheme for the image signature because instead of just coding scale, orientation would be recorded as well.



Extra Slides

Fingerprint Biometrics

In 1997, a Lucent-sponsored venture, Veridicom, was formed to commercialize solid-state fingerprint sensor systems, originally developed at Bell Labs.

There were many technical challenges during the course of my stay at this company. Two interesting pieces of work were:

1. Anti-spoof
2. Swipe sensor



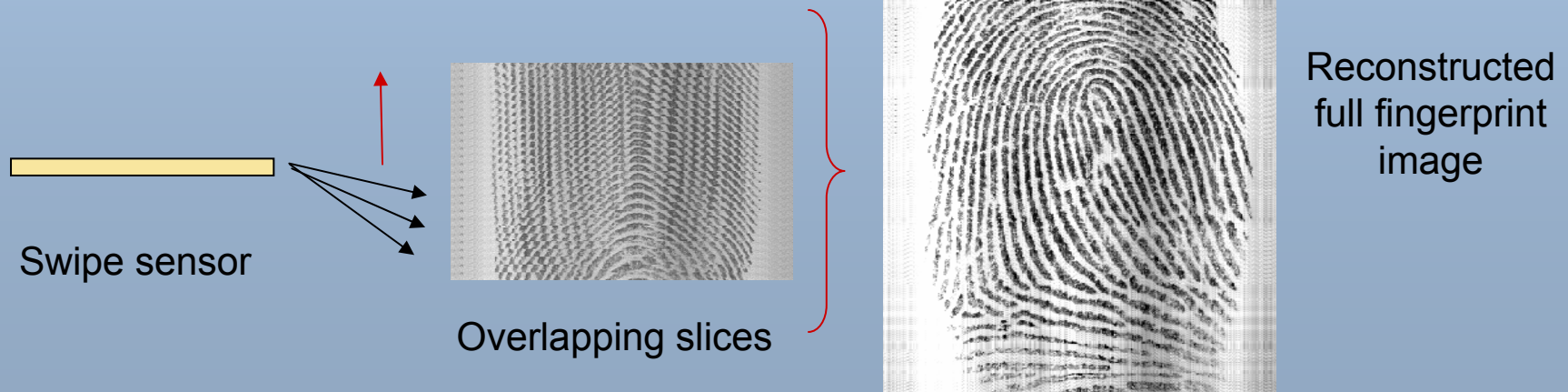
Fingerprint Biometrics

Swipe Fingerprint Sensor:

Instead of a full silicon sensor of size 250x300, cost and space can be saved by having a “swipe” sensor. This is an array of 8x300 (or smaller height) that the user has to swipe the finger down longitudinally. Overlapping images of sizes 8x300 are captured. These are aligned and reconstructed using the overlap information.

The major advantages are cost and size. Chip cost is roughly proportional to size, and these chips are about 30x smaller. Their smaller size enables placement on a cell phone or other small personal device.

The disadvantage is that the user must learn to swipe such that a good image is captured. This is a function of the user and the reconstruction algorithm.



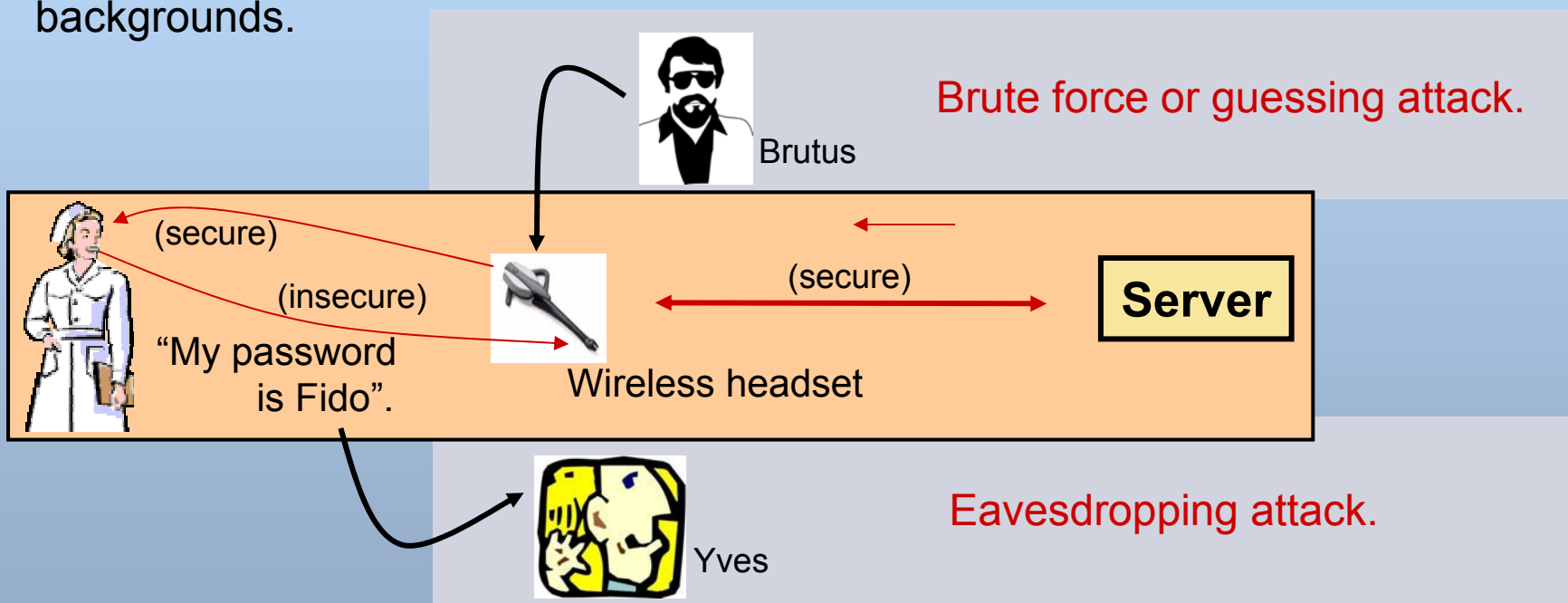
Extra Slides

How to Securely Speak an Authentication Secret

How can you authenticate verbally?

Hint 1: You can't use a password because of eavesdroppers.

Hint 2: We eliminate speaker verification because it is unreliable in noisy backgrounds.



Reference:

L. O'Gorman, L. Brotman, M. Sammon, "How to speak an authentication secret securely from an eavesdropper," 14th Int. Workshop on Security Protocols, Cambridge, England, March 2006.

How to Securely Speak an Authentication Secret

SPIN can be formalized as,

$$\text{SPIN}(m, c_D, c_I, L) \left\{ \begin{array}{l} m = \text{no. of memorized authentication substitutions} \\ c_D, c_I = \text{no. of camouflage elements, dependent and independent} \\ L = \text{no. of levels of an element} \end{array} \right.$$

Using this notation, we can determine the following equations that describe performance tradeoffs,

Length of authentication sequence:

Minimum: $n = m + c_D = L$ (i.e., $c_D = L - m$ for uniform challenge elements)

For added security: $n = m + c_D + c_I = L + c_I$

Security Strength:

Best case: $S_{max} = L(L-1)(L-2)\dots(L-m+1) = \binom{L}{m} m!$ (if don't consider Brutus attacks)

Worst case: $S_{min} = m!$ (with c_D elements but no c_I elements)

Actual case: can change S probabilistically between min and max by insertion of c_I →

How to Securely Speak an Authentication Secret

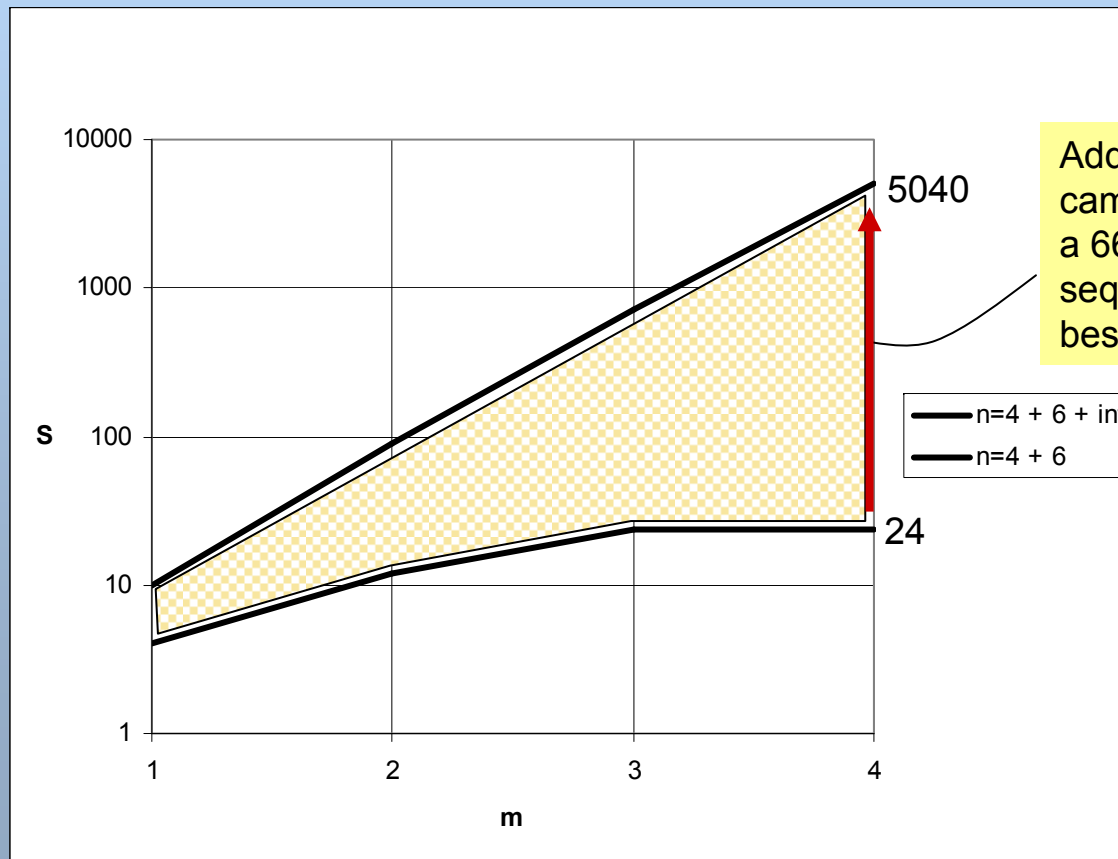
Conclusion:

- Method for authenticating securely by voice
- Secure with respect to eavesdropper
- Lower bounded security – both absolutely and probabilistically – with respect to brute force attacker
- Tradeoff is lower security strength and longer time to authenticate than regular password or PIN
- Tradeoffs are costly, but are there better alternatives?

How to Securely Speak an Authentication Secret

SPIN Tradeoffs – e.g., $m=4$, $c_d=6$, $L=10$

What number of c_i elements does it take to increase security strength from minimum to maximum with 66% probability?

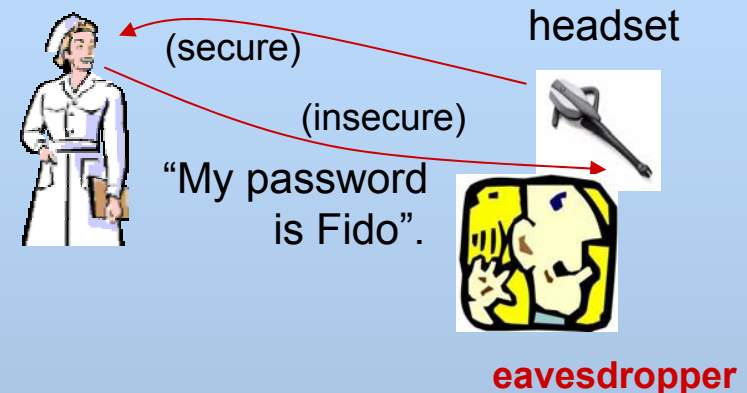


Adding $c_i=20$ extra camouflage elements gives a 66% likelihood that a sequence will have best-case security strength.

MACCS Security

How do you *speak* a password securely?

Challenge – There is no keyboard entry to MACCS and spoken commands can be overheard by eavesdroppers, so a traditional password or PIN cannot be used to authenticate users.



Two Options:

1. **SPIN (Spoken PIN)** – this is a substitution cipher method where the user memorizes color-number pairs and substitutes numbers for colors in the response to a challenge.

E.g., **challenge:** 1, *red*, *yellow*, 3, *blue*, 5 **response:** 1, 4, 6, 3, 2, 5

1. **QDP (Query-Directed Passwords)** – user responds to personal questions that are *known* rather than *memorized*. There are a few questions (2-4) each with multiple choices. This takes longer than SPIN, but requires no memorization.

E.g., **challenge 1:** "Color of car on which you learned to drive:
1 - red, 2 - green, 3 - white, 4 - black?" → **response:** "2" ...