Password Based Authentication Scheme: Safety and Usability Analysis

By
Samrat Mondal
Assistant Professor
Indian Institute of Technology Patna
Patna, Bihar, India
Outline

1. Basics of Authentication
   - Types of Authentication

2. Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3. Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4. Conclusions
Authentication

“Authentication is often the first line of defense against attack”

Figure: A Password Controlled Login Window Used for Authentication
Authentication

*Figure*: A Password Controlled Login Window Used for Authentication

“Authentication is often the first line of defense against attack”
Authentication

- confidentially binds an identity to a user.
- deals with the verification of someone’s identity.

Authentication is succeeded by the Access Control Mechanism.
Authentication

- confidentially binds an identity to a user.
- deals with the verification of someone’s identity.

Authentication is succeeded by the Access Control Mechanism
Outline

1 Basics of Authentication
   - Types of Authentication

2 Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3 Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4 Conclusions

By Samrat Mondal
Types of Authentication

Authentication is based on

1. Something the subject knows
2. Something that subject has
3. Something that the subject is
4. Somewhere the subject is
Types of Authentication

Authentication is based on

1. Something the subject knows
2. Something that subject has
3. Something that the subject is
4. Somewhere the subject is
Types of Authentication

Authentication is based on

1. Something the subject knows
2. Something that subject has
3. Something that the subject is
4. Somewhere the subject is
Types of Authentication

Authentication is based on

1. Something the subject knows
2. Something that subject has
3. Something that the subject is
4. Somewhere the subject is
Types of Authentication

Authentication is based on

1. Something the subject knows
2. Something that subject has
3. Something that the subject is
4. Somewhere the subject is
Something the subject knows

- Deals with the verification of someone’s secret.
- Secret such as *passwords*.
  - A password is some sequence of characters.
  - Something that nobody else can guess difficult in practice
Something the subject knows

- Deals with the verification of someone’s secret.
- Secret such as *passwords*.
  - A password is some sequence of characters.
  - Something that nobody else can guess
    difficult in practice
Outline

1. Basics of Authentication
   - Types of Authentication

2. Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3. Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4. Conclusions

By Samrat Mondal
Textual Passwords

- Suppose a password is 8 characters long.
- Each character has 256 possible choices.
- Then the possible passwords $256^8 = 2^{64}$.
- To find a password, an attacker will have to explore $2^{64}$ passwords.
Suppose a password is 8 characters long.
Each character has 256 possible choices.
Then the possible passwords $256^8 = 2^{64}$.
To find a password, an attacker will have to explore $2^{64}$ passwords.
Issues with Passwords

- However, the users do not select passwords at random.
- Users must remember their passwords.
- So a user is far more likely to choose an 8 character password such as security than, say, $kfyw*@8s$
- A clever attacker can make far fewer than $2^{64}$ guesses and have a high probability of successfully cracking a password.
Issues with Passwords

- However, the users do not select passwords at random.
- Users must remember their passwords.
- So a user is far more likely to choose an 8 character password such as *security* than, say, $kfYw* a@8s$
- A clever attacker can make far fewer than $2^{64}$ guesses and have a high probability of successfully cracking a password.
Nonrandomness of Passwords

• Thus a carefully selected “dictionary” of $2^{20} \approx 1,000,000$ passwords would likely give an attacker a reasonable probability of cracking a password.

• The probability of cracking a randomly selected password from the dictionary is $2^{20}/2^{64} = 1/2^{44}$

• Nonrandomness is thus a serious problem with passwords.
Nonrandomness of Passwords

- Thus a carefully selected “dictionary” of $2^{20} \approx 1,000,000$ passwords would likely give an attacker a reasonable probability of cracking a password.

- The probability of cracking a randomly selected password from the dictionary is $2^{20}/2^{64} = 1/2^{44}$

- Non-randomness is thus a serious problem with passwords.
Textual Passwords

Password

- Ideal passwords should be easy to remember but difficult to guess.
- Weak passwords *samrat*, *16122012*, *MondalSamrat*
- Strong passwords *jfIej* $\times 43j$ $-$ *EmmL* $+$ *y*, *0986437269523*, *1C1SStwelve*, *IhW11WC*
- *Passphrase* can be used to build a strong password.
Textual Passwords

Password

- Ideal passwords should be easy to remember but difficult to guess.
- **Weak passwords** *samrat, 16122012, MondalSamrat*
- **Strong passwords** *jfIej* $\ast 43j - EmmL + y, 0986437269523, 1C1SStwelve, IhW11WC*
- **Passphrase** can be used to build a strong password.
Ideal passwords should be easy to remember but difficult to guess.

Weak passwords: samrat, 16122012, MondalSamrat

Strong passwords: jfIej * 43j – EmmL + y, 0986437269523, 1C1SStwelve, IhW11WC

Passphrase can be used to build a strong password.
Password

- Ideal passwords should be easy to remember but difficult to guess.
- Weak passwords *samrat*, *16122012*, *MondalSamrat*
- Strong passwords *jfIej* *43j* − *EmmL* + *y*, *0986437269523*, *1C1SStwelve*, *IhW11WC*
- *Passphrase* can be used to build a strong password.
Password verification

- System must verify whether the entered password is correct or not
- So the system maintains all the correct passwords in a file
- But storing the raw passwords in a file is not a good idea as an attacker may target that
  - It is more secured to store hashed passwords
  - So if the entered password is $x$ and the hash function is $h$ then system stores $y$ which is equal to $h(x)$
Password verification

- System must verify whether the entered password is correct or not
- So the system maintains all the correct passwords in a file
- But storing the raw passwords in a file is not a good idea as an attacker may target that
- It is more secured to store hashed passwords
- So if the entered password is $x$ and the hash function is $h$ then system stores $y$ which is equal to $h(x)$
### Salt Value

- Let \( p \) be a given password
- A random salt \( s \) is generated and compute \( y = h(p, s) \)
- Now in the password file for each user, the pair \((s, y)\) is stored
- Salt \( s \) is not a secret
Objective of Adding Salt

- Suppose user A’s password is salted with $s_a$ and for user B the salt value is $s_b$.
- Now to crack A’s password using a dictionary, the attacker must compute hashes of words in his dictionary with salt value $s_a$.
- Similarly to crack B’s password using a dictionary, the attacker must compute hashes of words in his dictionary with salt value $s_b$.
- For password file with $N$ users the attacker’s work has increased by a factor of $N$. 
Password Cracking

Let’s us assume the followings

- All passwords are 8 characters in length
- There are 128 choices for each character
- So the possible no. of passwords is $128^8 = 2^{56}$
- Passwords are stored in a password file that contains $2^{10}$ hashed passwords
- Attacker has a dictionary of $2^{20}$ common passwords
- Attacker expects that any given password will appear in his dictionary with probability $1/4$
- Work for cracking password is measured by the no. of hashes computed (comparisons are ignored)
Password Cracking: Different Cases

1. Attacker wants to find the password of a particular user (say Mr. X) without using a dictionary of likely passwords.

2. Attacker wants to find the password of Mr. X using a dictionary of likely passwords.

3. Attacker wants to find any password in the hashed password file without using a dictionary.

4. Attacker wants to find any password in the hashed password file using the dictionary.
Password Cracking: Different Cases

1. Attacker wants to find the password of a particular user (say Mr. X) without using dictionary of likely passwords

2. Attacker wants to find the password of Mr. X using dictionary of likely passwords

3. Attacker wants to find any password in the hashed password file without using dictionary

4. Attacker wants to find any password in the hashed password file using the dictionary
Password Cracking: Different Cases

1. Attacker wants to find the password of a particular user (say Mr. X) without using dictionary of likely passwords

2. Attacker wants to find the password of Mr. X using dictionary of likely passwords

3. Attacker wants to find any password in the hashed password file without using dictionary

4. Attacker wants to find any password in the hashed password file using the dictionary
Password Cracking: Different Cases

1. Attacker wants to find the password of a particular user (say Mr. X) without using dictionary of likely passwords

2. Attacker wants to find the password of Mr. X using dictionary of likely passwords

3. Attacker wants to find any password in the hashed password file without using dictionary

4. Attacker wants to find any password in the hashed password file using the dictionary
### Textual Passwords

## Password Cracking: Different Cases

1. Attacker wants to find the password of a particular user (say Mr. X) without using dictionary of likely passwords

2. Attacker wants to find the password of Mr. X using dictionary of likely passwords

3. Attacker wants to find any password in the hashed password file without using dictionary

4. Attacker wants to find any password in the hashed password file using the dictionary
Case 1

Attacker wants to find the password of a particular user (say Mr. X) without using dictionary of likely passwords

- Precisely equivalent to an exhaustive key search
- The expected work is $2^{56}/2 = 2^{55}$
Case 2

Attacker wants to find the password of Mr. X using dictionary of likely passwords

- With probability $1/4$, the password of Mr. X will appear in dictionary
- Attacker would expect it to find it after hashing half of the words of the dictionary
- With probability $3/4$ the password is not in the dictionary
- Attacker would expect it to find using $2^{55}$ tries
- The expected work is $\frac{1}{4}(2^{19}) + \frac{3}{4}(2^{55}) \approx 2^{54.6}$
Case 3

Attacker wants to find any password in the hashed password file without using dictionary

- In this case the attacker will be satisfied to find any one of the $2^{10}$ passwords
- Attacker needs to make $2^{55}$ distinct comparisons before he expects to find a match
- Attacker takes each password and hashes it and then compares it with all the $2^{10}$ passwords
- The expected work is $\frac{2^{55}}{2^{10}} = 2^{45}$
Case 4

Attacker wants to find any password in the hashed password file using the dictionary

- The probability that at least one password is in the dictionary is
  
  \[ 1 - \left( \frac{3}{4} \right)^{1024} \approx 1 \]

- So we can safely ignore the case where no password in the file appears in attacker’s dictionary

- Thus the attacker needs to make only \( 2^{19} \) comparisons before he expects to find a password

- As each hash computation yields \( 2^{10} \) comparisons, so the expected work is \( 2^{19} / 2^{10} = 2^9 \)
Textual Passwords

Challenge Response

- Passwords are reusable.
- If an attacker sees a password he can replay it.
- The system cannot distinguish between the attacker and the legitimate user and allow access.
- Authenticate in such a way that the transmitted password changes each time.
- If the attacker replays the previously used password, the system will reject it.
Outline

1. Basics of Authentication
   - Types of Authentication

2. Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3. Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4. Conclusions
Graphical Passwords

Why Graphical Password?

To improve

- password memorability
- usability
- strength against guessing attacks
Graphical Password

- Like text password, graphical passwords are also knowledge based authentication mechanism.
- Unlike text password, graphical passwords puts less strain on human memory [10]
Graphical Passwords

Graphical Password: Memorability

It is based on memory task involved in remembering and entering the password [11]

1. Recall
2. Recognition
3. Cued recall
Graphical Passwords

Recall based

- Sometimes referred as *drawmetric* systems because users recall and reproduce a secret drawing [1]
- Recall is difficult memory task as retrieval is done without memory prompts or cues
- Example: DAS [9], BDAS [8]
Graphical Passwords

Recognition based

- Also known as *cognometric systems* [1] or *searchmetric systems* [6]
- Generally require that users memorize a portfolio of images during password creation
- During log in, he must recognize those images from among decoys
- Recognition based systems have been proposed using various types of images, most notably: faces, random art, everyday objects, and icons.
- Example: PassFaces [4], Story [5]
Cued recall based

- Cued-recall systems typically require that users remember and target specific locations within a presented image.
- This feature, intended to reduce the memory load on users, is an easier memory task than pure recall.
- Such systems may also be called *locimetric* [1] due to their reliance on identifying specific locations.
- Example: PassPoints [7]
Outline

1. Basics of Authentication
   - Types of Authentication

2. Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3. Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4. Conclusions
Attacks on Password Based Scheme

Graphical Password: Security

- Must ensure adequate security
- Must defend some common attacks
Graphical Password: Security Attacks

- Guessing attack
- Capture attack
Attacks on Password Based Scheme

Guessing attack

Attacker are able to
- Exhaustively search through the entire theoretical password space
- Predict the higher probable passwords
Attacks on Password Based Scheme

## Capture attack

Attackers directly obtain the passwords by

- **Shoulder surfing**
  - Credentials are captured by direct observation during the login process or through some recording device

- **Phishing**
  - A social engineering attack where users are tricked into entering their credentials

- **Malware**
  - Unauthorized software are installed on client computers or servers to capture keyboard, mouse or screen output which is then parsed to find login
Attacks on Password Based Scheme

Capture attack

Attackers directly obtain the passwords by

- **Shoulder surfing**
  - Credentials are captured by direct observation during the login process or through some recording device

- **Phishing**
  - A social engineering attack where users are tricked into entering their credentials

- **Malware**
  - Unauthorized software are installed on client computers or servers to capture keyboard, mouse or screen output which is then parsed to find login
Attacks on Password Based Scheme

Capture attack

Attackers directly obtain the passwords by

- **Shoulder surfing**
  - Credentials are captured by direct observation during the login process or through some recording device

- **Phishing**
  - A social engineering attack where users are tricked into entering their credentials

- **Malware**
  - Unauthorized software are installed on client computers or servers to capture keyboard, mouse or screen output which is then parsed to find login
Capture attack

Attacker directly obtain the passwords by

- **Shoulder surfing**
  - Credentials are captured by direct observation during the login process or through some recording device

- **Phishing**
  - A social engineering attack where users are tricked into entering their credentials

- **Malware**
  - Unauthorized software are installed on client computers or servers to capture keyboard, mouse or screen output which is then parsed to find login
Attacks on Password Based Scheme

Capture attack

Attackeres directly obtain the passwords by

- **Shoulder surfing**
  - Credentials are captured by direct observation during the login process or through some recording device

- **Phishing**
  - A social engineering attack where users are tricked into entering their credentials

- **Malware**
  - Unauthorized software are installed on client computers or servers to capture keyboard, mouse or screen output which is then parsed to find login
Capture attack

Attackers directly obtain the passwords by

- **Shoulder surfing**
  - Credentials are captured by direct observation during the login process or through some recording device

- **Phishing**
  - A social engineering attack where users are tricked into entering their credentials

- **Malware**
  - Unauthorized software are installed on client computers or servers to capture keyboard, mouse or screen output which is then parsed to find login
Outline

1 Basics of Authentication
   - Types of Authentication

2 Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3 Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4 Conclusions
Draw A Secret (DAS)

- Proposed by Jermyn et al. in 1999 [9]
- First recall based graphical password approach
- Users draw their password on a 2D grid using a stylus or mouse
A drawing may consist of one continuous pen stroke or preferably several strikes separated by “pen ups”

To log in users repeat the same path through the grid cells

The system encodes the user drawn password as the sequence of coordinates of the grid cells passed through in the drawing, yielding an encoded DAS password
Figure: Sample Draw-A-Secret Password
Working of DAS

- User draws a design on the grid using the stylus
- The drawing is mapped to a sequence of coordinate pairs
  - By listing the cells through which drawing passes in the order in which it passes through them
- A distinguishing coordinate is used for “pen up” event

The coordinate sequence of previous diagram is (2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5,5)
DAS Password

- A stroke is a sequence of cells which does not contain “pen up” event
- A password is defined to be a sequence of strokes separated by “pen up” events
- The length of a stroke is the number of coordinate pairs it contains
- The length of a password is the sum of the lengths of its component strokes (excluding the “pen-up” character)
DAS Password Space

- Users are equally likely to pick any element as their password.
- The raw size is an upper bound on the information content of the distribution that users choose in practice.
- For a 5 x 5 grid and maximum length 12, the theoretical password space has cardinality $2^{58}$
- Whereas the number of textual passwords of 8 characters constructed from the principle of ASCII codes $95^8 \approx 2^{53}$
DAS Analysis

- Superior memorability
- Users may prefer passwords with
  - Fewer strokes
  - Common shapes
  - Common letter
## Outline

1. Basics of Authentication
   - Types of Authentication

2. Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3. Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4. Conclusions
PassFaces

- One of the most studied recognition based system
- It is face recognition based scheme
Motivation

Motivation behind using face recognition scheme

- Infants are born with a capacity to recognize faces and show a preference for looking at faces well within the first hour after birth.
- Infants can recognize their mother after only two days.
- We know that we have seen a familiar face within twenty thousandths of a second (20ms).
- In one experiment people recognized schoolmates they had not seen for 35 years with over 90% accuracy.

Thus viewing a face is quite different from viewing any other object.
Motivation

Motivation behind using face recognition scheme

- Infants are born with a capacity to recognize faces and show a preference for looking at faces well within the first hour after birth.
- Infants can recognize their mother after only two days.
- We know that we have seen a familiar face within twenty thousandths of a second (20ms).
- In one experiment people recognized schoolmates they had not seen for 35 years with over 90% accuracy.

Thus viewing a face is quite different from viewing any other object.
PassFaces

Working Methodology

- Users pre-select a set of human faces
- During login, a panel of candidate face is presented
- Users must select the face belonging to their set from among decoys
- Several such rounds are repeated with different panels
- Each round must be executed correctly for a successful login
Working Methodology (contd.)

- In the original system 9 images are used per panel
- User pre-selects 4 faces
- During login, the Passfaces are presented to the user, one at a time, in a $3 \times 3$ face grid that contains the assigned Passface and 8 decoys
  - Use of $3 \times 3$ grid allows Passfaces to be used on devices such as ATMs and Web TVs where this may be the only means of user input.
- If the user selects the PassFaces correctly in all the 4 occasions then the login is successful
PassFaces Images

Figure: Sample Panel of PassFace Login Screen
PassFaces Login
Password Space

- The theoretical password space for PassFaces is \( M^n \)
- Now 9 faces per panel will give \( M = 9 \)
- User pre-selects 4 faces so \( n = 4 \)
- Thus password space of the system is \( 9^4 = 6561 \approx 2^{13} \)
PassFaces

Features

- Can’t be written down or copied
- Can’t be given to another person
- Can’t be guessed
- Involve cognitive not memory skills
- Can be used as a single or part of a dual form of authentication
PassFaces

Analysis

- Users often select predictable faces like “smiling”, “attractive”, etc.
- Password creation time may be large
  - As the user may take a lot of time to select faces from a large pool of faces
  - Password creation often takes 3 to 5 minutes
- Less vulnerable to social engineering attack
  - As the system strategically selects similar decoys
  - Also correctly describing a portfolio image is not an easy task
PassFaces

Analysis

- Users often select predictable faces like “smiling”, “attractive”, etc.
- Password creation time may be large
  - As the user may take a lot of time to select faces from a large pool of faces
  - Password creation often takes 3 to 5 minutes
- Less vulnerable to social engineering attack
  - As the system strategically selects similar decoys
  - Also correctly describing a portfolio image is not an easy task
Analysis

- Users often select predictable faces like “smiling”, “attractive”, etc.
- Password creation time may be large
  - As the user may take a lot of time to select faces from a large pool of faces
  - Password creation often takes 3 to 5 minutes
- Less vulnerable to social engineering attack
  - As the system strategically selects similar decoys
  - Also correctly describing a portfolio image is not an easy task
Users often select predictable faces like “smiling”, “attractive”, etc.

Password creation time may be large
- As the user may take a lot of time to select faces from a large pool of faces
- Password creation often takes 3 to 5 minutes

Less vulnerable to social engineering attack
- As the system strategically selects similar decoys
- Also correctly describing a portfolio image is not an easy task
Outline

1. Basics of Authentication
   - Types of Authentication

2. Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3. Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4. Conclusions
S3PAS

Scalable Shoulder Surfing Resistant Textual-Graphical Password Authentication Scheme

- Proposed by Zhao and Li in 2007 [2]
- Designed to be used as a client server environment
- Shoulder Surfing Resistant
- Matches the conventional passwords
- Robust against brute force attack
- Supports both keyboard and mouse as input devices
S3PAS System

- Initially S3PAS generates the login image
- The image contains a set of printable characters (say $T$) used in conventional passwords
- Typically $|T| = 94$
- $T^*$ denotes all the combination consisting of the elements in $T$
  - $T^*$ is also the password space
- An original password $k$ is an element of $T^*$
  - $|k|$ denotes the length of the password
S3PAS Login

Figure: S3PAS Login Screen and Login Image
S3PAS Login Process

- The system initially scatters the set $T$ in the login image
- To login the user must find (but should not point) all his original password characters in the login image
- Now considering three characters at a time of the original password, the user can visualize a triangle
  - These triangles are known as “Pass triangles”
- Click rule: The user is now required to click a character inside that invisible triangle
  - This character is known as “session pass character”
  - All such session pass characters form the “session password”
S3PAS Login Example

- Let the original password k is “A1B3”
- As $|k| = 4$ so the following four pass triangles to be considered
  - “A1B”, “1B3”, “B3A” and “3A1”

Figure: Pass triangle for $\triangle A1B$ and $\triangle 1B3$
S3PAS Login Process

**Figure:** Pass triangle for $\triangle B3A$ and $\triangle 3A1$

<table>
<thead>
<tr>
<th>Pass triangles</th>
<th>A1B</th>
<th>1B3</th>
<th>B3A</th>
<th>3A1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible session character</td>
<td>P</td>
<td>D</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>
Let’s consider the following scenarios

1. If two of those three pass characters are the same
   - A triangle cannot be constructed
   - However, an invisible line can be constructed
   - The user can select a character lying on that line as session character

2. If all the characters are same
   - Only a single character
   - The user can select a character from a certain circle area centred around that character
S3PAS Different Login Scenarios

Let’s consider the following scenarios

1. **If two of those three pass characters are the same**
   - A triangle cannot be constructed
   - However, an invisible line can be constructed
   - The user can select a character lying on that line as session character

2. **If all the characters are same**
   - Only a single character
   - The user can select a character from a certain circle area centred around that character
Let’s consider the following scenarios

1. **If two of those three pass characters are the same**
   - A triangle cannot be constructed
   - However, an invisible line can be constructed
   - The user can select a character lying on that line as session character

2. **If all the characters are same**
   - Only a single character
   - The user can select a character from a certain circle area centred around that character
### S3PAS Different Login Scenarios

Let’s consider the following scenarios:

1. **If two of those three pass characters are the same**
   - A triangle cannot be constructed
   - However, an invisible line can be constructed
   - The user can select a character lying on that line as session character

2. **If all the characters are same**
   - Only a single character
   - The user can select a character from a certain circle area centred around that character
Let’s consider the following scenarios

1. **If two of those three pass characters are the same**
   - A triangle cannot be constructed
   - However, an invisible line can be constructed
   - The user can select a character lying on that line as session character

2. **If all the characters are same**
   - Only a single character
   - The user can select a character from a certain circle area centred around that character
S3PAS Analysis: Shoulder Surfing Attack

Shoulder Surfing Attack

- If the attacker observes or records the pass characters
  - It will be difficult to gain enough information about the original password

- However, as two consecutive “pass triangles” have common border so the attacker may exploit that fact
S3PAS Analysis: Shoulder Surfing Attack

Shoulder Surfing Attack

- If the attacker observes or records the pass characters
  - It will be difficult to gain enough information about the original password

- However, as two consecutive “pass triangles” have common border so the attacker may exploit that fact
S3PAS Analysis: Shoulder Surfing Attack

Shoulder Surfing Attack
- If the attacker observes or records the pass characters
  - It will be difficult to gain enough information about the original password
- However, as two consecutive “pass triangles” have common border so the attacker may exploit that fact
S3PAS Analysis: Random Click Attack

- Attackers have the chance to click on the right areas just by random click.
- If the size of the pass triangles area are too large then the success of random click attack increases.
- For a password of length $k$, the probability of get authentication just by random click is $0.076^{|k|}$.
- So for a password of length 4, the probability will be approx. $0.076^{|k|} \approx 0.0000334$. 
S3PAS Analysis: Random Click Attack

- Attackers have the chance to click on the right areas just by random click
- If the size of the pass triangles area are too large then the success of random click attack increases
- For a password of length $k$, the probability of get authentication just by random click is $0.076^k$
- So for a password of length 4, the probability will be approx. $0.076^4 \approx 0.0000334$
S3PAS Analysis: Brute Force Attack

- Traditionally brute force attack can be tackled using a sufficiently large password space
- Here the password space is dependent on $|T| = 94$
- This is sufficiently large
- Use of enhanced graphical scheme will increase the password space
- “Change image” technology
  - the image will be changed if a user fails in clicking the correct areas, or inputs wrong session passwords for more than a certain no. of times
S3PAS Analysis: Brute Force Attack

- Traditionally brute force attack can be tackled using a sufficiently large password space.
- Here the password space is dependent on $|T| = 94$.
- This is sufficiently large.
- Use of enhanced graphical scheme will increase the password space.
- “Change image” technology:
  - the image will be changed if a user fails in clicking the correct areas, or inputs wrong session passwords for more than a certain no. of times.
S3PAS Enhancements

1. Three set scheme to avoid "common border problem"
2. Rule Based Scheme
3. Graphical icons instead of textual icons
S3PAS

Three Set Scheme

- In the single set S3PAS scheme, the consecutive images share a common border.
- By analysing minutely, the common border may help an attacker to guess the correct session character.
- Three set scheme is a possible alternative to avoid this problem:
  - Randomly scatter three copies of the set T in the login image.
  - Then there will be $94 \times 3 = 282$ characters in the login image.
  - To distinguish characters in different sets, color can be used.
Rule Based Scheme

- Users are allowed to define their own “Pass Rules”
- So no need to follow the same “Click Rule”
- The “Pass Rule” will remain unknown to the attacker also
- This will make the job of the attacker more difficult
Enhanced Graphical Scheme

To increase the password space
- Include “image icons” instead of all the printable characters
- Similar concepts are available in Sobrado and Birget’s work
Outline

1. Basics of Authentication
   - Types of Authentication

2. Password based Authentication
   - Textual Passwords
   - Graphical Passwords
   - Attacks on Password Based Scheme

3. Existing Techniques
   - DAS
   - PassFaces
   - S3PAS
   - SSSL

4. Conclusions
SSSL: Shoulder Surfing Safe Login

- Proposed by [Perkovic et al., SoftCom, 2009] [3]
- It is a challenge response protocol
- Used as a partially observable model
- Claimed to be user friendly and cost efficient
Secure PIN Entry with SSSL

SSSL comprises three major components:

1. A protected channel
2. An SSSL table
3. A set of response buttons
SSSL Table

<table>
<thead>
<tr>
<th></th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure**: SSSL Tables

<table>
<thead>
<tr>
<th>K_7</th>
<th>K_8</th>
<th>K_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>K_4</td>
<td>K_5</td>
<td>K_6</td>
</tr>
<tr>
<td>K_1</td>
<td>K_2</td>
<td>K_3</td>
</tr>
</tbody>
</table>

**Figure**: Mapping of SSSL Response Table
Working Methodology

- Let the secret pin be 46548
- At time $t_0$ the user receives a challenge say $c_0$ from 1, \ldots, 9
- User then looks up the yellow area and locates (visually) the first digit of the PIN
- User then locates the challenge $c_0$ in the immediate neighbourhood of the previously located digit
- User then answers the challenge by clicking the response button that shows the relative position of the challenge
SSSL

Example

Figure: SSSL Tables

<table>
<thead>
<tr>
<th>time</th>
<th>$t_0$</th>
<th>$t_1$</th>
<th>$t_2$</th>
<th>$t_3$</th>
<th>$t_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Challenge Values</td>
<td>9</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>User’s response</td>
<td>$k_1$</td>
<td>$k_5$</td>
<td>$k_8$</td>
<td>$k_8$</td>
<td>$k_9$</td>
</tr>
</tbody>
</table>
Usability Aspects

- Easy to learn and use for a novice user
- User does not require any numerical computation
- The no. of challenge response is equal to the size of the PIN
- The average login time is around 8 seconds
The size of the PIN space

- Allows only 9 digits thus reduces PIN entropy
- Use of longer PIN
- If the minimum PIN length is 5 then PIN space is $9^5 > 10^4$ which is the classical 4 PIN solution
Security Analysis

Let’s assess the security of SSSL based on followings:

- Camera Recording (Passive) Adversary
- Side Channel Timing Attacks
- Active Attacks
Camera Recording Adversary

- The attacker will try to learn the PIN just by recording the SSSL login procedure.
- Here attacker is passive and does not interact with the system.
- Two analysis:
  1. The challenge value remains unknown during the login phase.
  2. Eavesdropping on the protected channel.
Let $d$, $c$ and $r$ denote secret PIN digit, challenge value and response

Let $d = 4$, $c = 9$ and so $r = k_1$

Now what does attacker learn by observing the response?

If $d$ and $c$ remain secret, then attacker can understand that the one of the following nine $(d, c)$ pairs has been used

- $d = 4$, $c = 9$
- $d$, $c$, $r$, $k_1$
Let $d$, $c$ and $r$ denote secret PIN digit, challenge value and response.

Let $d = 4$, $c = 9$ and so $r = k_1$.

Now what does attacker learn by observing the response?

If $d$ and $c$ remain secret, then attacker can understand that the one of the following nine $(d, c)$ pairs has been used.
Unknown Challenged Value

Figure: SSSL Tables
Unknown Challenge Value (contd.)

- Both $d$ and $c$ are selected randomly from $1, \ldots, 9$
- Thus each of the above pairs $(d, c)$ is equally likely to be true pair
- So the attacker learns nothing about the secret PIN digit $d$ and also $c$
Eavesdropping on The Protected Channel

- If the attacker can find the challenge value then he can find the secret PIN
- So the attacker may try to attack the protected channel
- If the challenge is generated using audio and the user receives it through earphones
  - The attacker can use a parabolic reflector to collect sound energy produced by earphones
  - This threat can be mitigated by reducing sufficiently the volume level of an audio challenge
  - Some other advanced sound and noise reduction techniques can also be used
Eavesdropping on The Protected Channel

- If the attacker can find the challenge value then he can find the secret PIN
- So the attacker may try to attack the protected channel
- If the challenge is generated using audio and the user receives it through earphones
  - The attacker can use a parabolic reflector to collect sound energy produced by earphones
  - This threat can be mitigated by reducing sufficiently the volume level of an audio challenge
  - Some other advanced sound and noise reduction techniques can also be used
Side Channel Timing Attack

- A timing attack
- A common attack to any cognitive authentication scheme that involves the human user
- The attacker tries to analyze from the time the system takes to execute a particular operation
- Assume that attacker has the capability to record the user’s reaction time
Side Channel Timing Attack (contd.)

Figure: Patterns showing different response times by two users with PINs: 46548 and 73827
Analyzing the Patterns

The attacker can extract some secret from the patterns

- For the first user, the patterns corresponding to first and fourth PIN digits are highly correlated
- Similarly, for the second user, the patterns corresponding to the first and last PIN are highly correlated
- Thus the attacker can conclude that the respective PIN digits are same
- This reduces the security factor from $9^5$ to $9^4$ (i.e., approximately 89%)
- To mitigate this threat some random delay can be introduced
- Of course this will increase the login time
Active Attacks

- The attacker can trick the user to login from a compromised computer
- SSSL can easily be broken in such case
- A safe way to protect against such attack is completely bypassing the compromised computer
- Assume an end server authenticates the user who is connected to the server through the compromised computer
- If the end server is not compromised then the challenge can be provided directly by the end server
- *Tamper resistant microprocessor* can be used in this context
Conclusions

- Various password based graphical authentication schemes were discussed.
- Each scheme has its own usability and safety issues.
- Many of these schemes are vulnerable to shoulder surfing attack and having longer login time.
- So an authentication scheme which can balance the above two factors is on a high demand.
References

A. De Angeli, L. Coventry, G. Johnson, and K. Renaud
Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems
*International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 128-152, 2005

H. Zhao and X. Li
S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme
*21st International Conference on Advanced Information Networking and Applications Workshops*, 2007
References II

T. Perkovic, M. Cagali and N. Rakic
SSSL: Shoulder Surfing Safe Login
Software Telecommunications and Computer Networks, pp. 270-275, 2009

Passfaces Corporation
The science behind Passfaces
http://www.passfaces.com/enterprise/resources/white_papers.htm, 2009

D. Davis, F. Monrose, and M. Reiter
On user choice in graphical password schemes
13th USENIX Security Symposium, 2004
References

K. Renaud
Guidelines for designing graphical authentication mechanism interfaces.

S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon
PassPoints: Design and longitudinal evaluation of a graphical password system.
P. Dunphy and Y. Jan
Do background images improve “Draw a Secret” graphical passwords?

I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin,
The design and analysis of graphical passwords
8th USENIX Security Symposium, August 1999.

A. Paivio
Mind and Its Evaluation: A Dual Coding Theoretical Approach
Lawrence Erlbaum: Mahwah, N.J., 2006
References V

J.G. Raaijmakers and R.M. Shifrin
Models for recall and recognition
Annual Reviews Psych, Vol. 43, pp. 205-234, January 1992

M. Stamp.
Information Security.
Wiley.
Questions?
THANK YOU