Entering Passwords on a Spyware Infected Machine

Dinei Florencio and Cormac Herley
Microsoft Research
ABSTRACT
We examine the problem of entering sensitive data, such as passwords, from an untrusted machine (i.e., possibly infected with spyware). Using such a machine is obviously undesirable, and yet roaming users often have no choice. We consider whether it is possible to enter data to confound spyware assumed to be running on the machine in question. The difficulty of mounting a collusion attack on a single user’s password makes the problem more tractable than it might appear. We explore several approaches. In the first, we show how the user can embed a password in random keystrokes to confuse spyware, while leaving the actual login unaffected. In the second we employ a proxy server to strip random keys. In the third we again employ a proxy that inverts a key mapping performed by the user. We examine also several potential attacks.
Motivation

- Accessing your accounts when roaming;
- Available terminal (kiosks, internet cafes) may be compromised; keyloggers a common risk.
- “Simply do not use” is not always an option.

Assumption:

- Terminal is running a keylogger.
A simple solution...

- Go to the login page;
- Click on Password (PWD) field;
- Type first character of PWD;
- Click outside PWD field;
- Type random characters (these will be ignored by the browser, but recorded by keylogger);
- Repeat until typing all PWD characters...
- Keylogger gets password interspersed with random characters.
... and a simple attack

- Replace keylogger with one that also records mouse click events ...
Assumptions / Requirements

- Attackers record everything you do, and everything on the screen;
- Plug-ins may access whatever goes over a SSL connection;
- No changes to the Bank login server;
- No changes to your daily logins;
- No password uploading/maintaining.
Is the problem possible?

- everything you see on the screen, and everything you type, is available to the attacker...

To our advantage:

- Collusion between different locations is hard;
- We are allowed to use a proxy server;
Basic Idea

- Use a separate channel (e.g., a safe terminal) to set up a **shared secret** with a login proxy server (MITM proxy);
  - NOTE: a *different* unsafe terminal is also ok, as long as we can assume no collusion between terminals.
  - NOTE2: the MITM proxy breaks the SSL connection;

- Use the proxy server to connect you to your desired site. Proxy is going to instruct you on how to modify/code your PWD, based on the shared secret.
Three alternatives

- METHOD 1: Minimum setup (3A

- METHOD 2: easiest to use (MyPics).

- METHOD 3: maximum security (print table).
METHOD 1 (least initial setup)

Before using:

› setup a username (no PWD), and inform any “non-usual” sites you may want to visit
› Receive (and memorize/keep) a shared secret consisting of a table position and a symbol (e.g., 3A❤️)
Login w/ method 1

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>♦</td>
<td>♠</td>
<td>♦</td>
<td>♠</td>
<td>♦</td>
<td>♠</td>
<td>♦</td>
<td>♠</td>
<td>♦</td>
<td>♠</td>
<td>♦</td>
<td>♠</td>
<td>♦</td>
<td>♠</td>
<td>♦</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>♣</td>
<td>♠</td>
<td>♣</td>
<td>♠</td>
<td>♣</td>
<td>♠</td>
<td>♣</td>
<td>♠</td>
<td>♣</td>
<td>♠</td>
<td>♣</td>
<td>♠</td>
<td>♣</td>
<td>♠</td>
<td>♣</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>♧</td>
<td>♠</td>
<td>♧</td>
<td>♠</td>
<td>♧</td>
<td>♠</td>
<td>♧</td>
<td>♠</td>
<td>♧</td>
<td>♠</td>
<td>♧</td>
<td>♠</td>
<td>♧</td>
<td>♠</td>
<td>♧</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td>♠</td>
<td>♤</td>
<td></td>
</tr>
</tbody>
</table>
Login w/ method 1
Login w/ method 1
### Login w/ method 1

![Password Page](image)

- **Password**: [ ]

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
</tr>
<tr>
<td>5</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td>♠️</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td>♦️</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td>♣️</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
<td>♥️</td>
</tr>
</tbody>
</table>
Login w/ method 1

![Password Page](Image)

<p>| | | | | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>♣️</td>
<td>♠️</td>
<td>✷️</td>
<td>♦️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
</tr>
<tr>
<td>2</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
</tr>
<tr>
<td>3</td>
<td>♦️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
</tr>
<tr>
<td>4</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
</tr>
<tr>
<td>5</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
</tr>
<tr>
<td>6</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
</tr>
<tr>
<td>7</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
</tr>
<tr>
<td>8</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
<td>♣️</td>
<td>♠️</td>
</tr>
</tbody>
</table>
Login w/ method 1
A few problems with METHOD 1

- Not safe enough: for a 8x16 table with 5 symbols, there are 640 options, entropy or visual inspection on these options may reveal the actual password;
- The Mouse problem: Several users left the mouse pointing at their assigned table location.
- The collusion problem: about 80% of users mistyped the password, and had to retype.
Before using:

- setup a username (no PWD), and inform any "non-usual" sites you may want to visit
- Upload some personal images/pictures
Welcome to SafeLogin.

In wartime, truth is so precious that she should always be attended by a bodyguard of lies.

- W. S. Churchill

URL of the login page :

Login Name :

Next>>
Welcome to SafeLogin.

In wartime, truth is so precious that she should always be attended by a bodyguard of lies.

- W. S. Churchill

URL of the login page: login.live.com

Login Name: ft_256@hotmail.com

Next>>
Obfuscated Password:

Type next character of password when you see one of your images. Otherwise type a random character.
Obfuscated Password: m

Type next character of password when you see one of your images. Otherwise type a random character.
Obfuscated Password: ma

Type next character of password when you see one of your images. Otherwise type a random character.
Obfuscated Password: mas

Type next character of passwd when you see one of your images. Otherwise type a random character.
Obfuscated Password: masdj3s0la(kf4mx94

Type next character of password when you see one of your images. Otherwise type a random character.
Sign in

Sign in now to view or change your account settings.

To sign in to the website where you clicked the Account Services link, click the Back button in your browser, and then sign in on the previous page.

Related links
- Sign up for an account
- Learn more about privacy and security
- Get answers from Customer Support
A few points about METHOD 2

- Safer than Method 1, but entropy still not as high as original password (only need to figure out which characters are part of password, about ~3 bits per character);
- Success rate above 95%.
METHOD 3 (safest)

Before using:

› Request a UserNumber, and inform any “non-usual” sites you may want to visit;
› Download and print an encryption table for future use.
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| a | t | C | j | J | L | 3 | R | X | k | J | K | a | c | 7 | V | g | F | x | U | k | 3 | f | m | n | Y | o | u | U | d | z | a |
| e | c | h | X | d | z | s | 3 | B | h | m | D | L | W | b | h | N | T | P | K | 8 | v | 4 | K | o | p | s | Q | E | f | T | o | e |
| l | a | S | u | c | 5 | V | w | s | B | K | s | k | p | k | H | p | y | a | y | W | 3 | U | G | i | u | x | K | M | f | l |
| n | z | 6 | J | B | 4 | 8 | x | M | P | U | 6 | f | K | E | d | k | k | 2 | g | P | r | Q | 3 | K | v | 6 | p | x | 4 | A | n |
| o | K | 5 | 5 | u | M | 5 | Y | y | b | D | t | Z | s | 5 | v | t | c | Y | B | t | f | v | E | R | W | 5 | 6 | g | w | o |
| p | e | K | d | j | q | 9 | U | g | F | Q | g | 5 | 2 | q | Q | b | 3 | 4 | e | K | S | 5 | n | y | c | f | w | i | X | Y | p |
| q | m | F | L | p | F | I | u | q | U | Y | u | y | N | W | u | h | j | w | j | e | 0 | 7 | u | K | J | B | s | M | h | V | h | q |
| r | i | 3 | E | y | N | 3 | i | 3 | X | r | P | c | 9 | D | z | i | K | F | i | k | U | V | u | d | d | j | r | f | 7 | r |
| s | V | a | y | U | 9 | r | M | m | Z | n | e | K | h | v | R | q | u | o | 2 | g | 0 | 8 | S | L | N | U | a | b | V | s |
| t | s | P | Z | r | b | t | f | h | c | o | D | S | H | 9 | 2 | y | 6 | Z | n | c | i | 2 | p | B | H | R | k | N | t |
| y | n | 4 | Y | h | A | 6 | 8 | 6 | E | V | E | o | m | t | p | 7 | 7 | B | x | o | T | G | B | N | C | f | 8 | 8 | R | U | y |
| G | h | F | S | L | J | y | 3 | E | r | f | 9 | u | L | 8 | E | U | m | N | H | R | z | x | y | m | o | j | Z | W | c | M | G |
| S | L | 7 | b | s | U | A | N | 7 | W | i | Y | i | b | k | T | S | Q | 9 | R | t | d | j | q | v | t | y | e | q | w | S | l |
| 1 | G | B | P | 7 | Q | c | Z | x | E | X | B | s | g | Y | 5 | e | R | 7 | N | u | N | f | t | E | E | y | A | s | n | 1 |
| 2 | f | x | i | t | t | X | r | L | P | Q | R | t | Y | y | w | g | Y | v | g | c | a | a | f | 9 | c | h | U | L | 2 |
| 3 | d | n | c | K | h | B | H | L | H | H | j | 8 | q | e | i | J | G | d | U | b | Q | p | A | z | J | A | v | j | D | 3 |
| 7 | S | t | S | 7 | b | W | k | R | f | 4 | y | X | h | E | d | 5 | h | J | V | m | t | U | w | p | 6 | L | E | 6 | 7 |
| & | 4 | X | 3 | G | i | t | T | 2 | 9 | m | m | g | j | 0 | 4 | q | J | Q | W | j | B | f | d | W | f | T | 5 | Q | u | & |
| % | Y | M | r | i | 8 | 3 | E | v | 3 | E | G | 7 | m | d | D | p | d | Z | B | w | j | s | Q | g | i | T | j | g | % |
| ) | D | N | F | T | a | 9 | i | s | j | T | T | e | 9 | r | p | R | S | 5 | G | v | 2 | c | c | P | U | P | o | w | Z | )

Table ID: 32780567
for 3rd password character, use column: 13
A few points about METHOD 3

- Entropy ~ as high as original password;
- Success rate around 75%, but collision not a problem anymore;
- Harder to use of all three;
- Requires pre-printing encryption table.
Implementation

1. Contact KLASSP webserver
2. Send userid, url
3. User inputs obscured password
4. Send obscured password
5. Request www.bigbank.com/login
6. Populate login form with actual userid, “roguePwd”
7. User clicks “submit”
8. Send userid, password
9. Replace “roguePwd” with actual password

Done
Future work

- Implement as reverse proxy, ie, be able to type 
  `http://proxy:port/www.cnn.com` to go to cnn through the proxy.

- NOTE: right now need to change the settings in the browser to point at the proxy.
Conclusions

- Shared-secret Proxy helps make it harder to capture passwords.
- No prior uploading of PWDs;
- Little setup or maintenance;
- Never 100% safe.
References


