User Authentication

The purpose of these activities is to introduce students to the issues that arise in authentication. Authentication, or the act of proving that someone is who they say they are, is one of the most common and important security tasks that users encounter. Users must prove their identity many times a day, whether online (to websites), to their devices (for instance, unlocking their mobile phone), or to other devices (such as ATMs).

The most common method of authentication is passwords, and in this module, we help students explore what makes a secure password, and how hackers attack passwords (and how to defend against those attacks). We introduce students to the three types of authentication (something you have, something you know, and something you are), with activities examining biometrics, alternative password schemes (graphical passwords), and authentication recovery methods.

At the end of this module, students should know what authentication is and how we authenticate. They should be able to list the three types of authentication, and explain how they are different. They will learn how to choose good passwords, and be introduced to threats affecting passwords and the relevant defences. They will explore new password technologies, including biometrics and graphical passwords. By exploring the relevant security issues, this unit will help build mental models of security and provide students with the knowledge to behave more securely in their real lives.

Introduction

Slide deck introducing authentication:

- What does it mean to authenticate?
- How do we authenticate in real life? On the telephone?
- Concept of shared secret
- Three types of authentication

Supplemental materials to accompany Stobert, E., Cavar, E., Malisa, L. and Sommer, D. (2017) Teaching Authentication in High Schools: Challenges and Lessons Learned. 2017 USENIX Workshop on Advances in Security Education.

Creating Good Passwords

In this activity you will learn about how to choose secure passwords.

Go to https://howsecureismypassword.net/
This site will let you test the strength of various passwords. It gives you an estimate of how long it would take an attacker to guess those passwords.

Try some sample passwords. How long does it take to guess each of these passwords?

password ____________________
password123 ____________________
pässwörd ____________________
estimate ____________________
01081291 ____________________
qwertzuiop ____________________
D1tt5U3 ____________________
Tr0ub4dour&3 ____________________
chuchichaeschtli ____________________
correcthorsebatterystaple ____________________
correct horse battery staple ____________________
n3k05uxu_phxsym ____________________

Imagine that you are picking new passwords, and they must conform to each of the rule sets listed below. For each set of rules, what is the strongest password that you can choose? What is the weakest password you can choose? (do not try your real passwords!)

Rule:	**Strongest password**:	**Weakest password**:
Up to 8 characters	________________	________________
At least 8 characters	________________	________________
At least 16 characters	________________	________________
Between 8 and 16 characters	________________	________________
At least 8 characters with no dictionary words	________________	________________
At least 8 characters, with at least one lowercase letter, one uppercase letter, one symbol, one digit, and no dictionary words	________________	________________
At least lowercase letter, one uppercase letter, one digit, and one special character (#,-./:=?@[]^{}~)	________________	________________
Up to 32 characters, no dictionary words longer than 4 letters	________________	________________

Supplemental materials to accompany Stobert, E., Cavar, E., Malisa, L. and Sommer, D. (2017) Teaching Authentication in High Schools: Challenges and Lessons Learned. 2017 USENIX Workshop on Advances in Security Education.

Even though there are many possible passwords of up to 8 characters, in the activity you saw that "password" could be guessed instantly. Why do you think this is?

Why do you think a password like "01081291" is guessed quickly?

A password like "qwertzuiop" is not a word at all, but can still be guessed quickly. Why?

The word "chuchichaeschtli" is a stereotypical Swiss word, but is considered by the website to be a strong password. Why?

List three characteristics of a strong password:

List three characteristics of a weak password:

Password Cracking

In this activity you will learn about how attackers hack into accounts by guessing passwords. You will pretend to be guessing passwords to access bank accounts.

Imagine you are a hacker trying to steal money from a local bank. You have gained access to the list of passwords for bank accounts, but the passwords have all been disguised. However, you know how the bank disguised their passwords, so you are able to guess PINs and see if they correspond to the passwords in the list.

You know that all passwords are 4-digit PINs (i.e., use only numbers 0-9). How many of the passwords on the list can you guess?

Go to (Link available upon request) to try your guesses and see if they match any of the passwords on your list.

Hint: Try patterns on the number pad, dates, or easy-to-remember numbers.

Password	**PIN**	**Password**	**PIN**
ABAC		CEDD	
ADED		CEEB	
BBAB		CEEE	
BCCF		DCBD	
BEBC		DFFF	
CAAB		ECDC	
CBBD		ECEE	
CBDC		ECFA	
CBFA		EEAE	
CCFD		EEFF	

A brute-force attack is when an attacker tries to guess all passwords in order, beginning with the first possible password (e.g., 0000) and going to the last (e.g. 9999).

a) What are two advantages of this method?

b) What are two disadvantages?

A dictionary attack is when an attacker starts by guessing the most popular passwords first (e.g. 1234), and then guesses the less popular passwords (in descending order of popularity).

a) What are two advantages of this method?

b) What are two disadvantages?

What strategy did you use to guess the passwords in the list? How many passwords were you able to guess?

How many possible 4-digit PINs are there? Show how you worked out your answer.

In this activity, you were allowed as many guesses as you like. If you went to a login page and tried the same activity, why wouldn't it work?

Based on your experience guessing these passwords, list two reasons it might be a good idea to assign random passwords to users.

Thinking about your own experiences with passwords, list two disadvantages of assigned random passwords.

Personal Knowledge Questions

Passwords are not the only method of authentication. If someone forgets their password, *recovery authentication* is used to prove that someone is who they say they are and give them access to their account.

In this activity, you'll learn about personal knowledge questions, which are one form of recovery authentication. They ask questions that should be easy for the real person to answer, but difficult for another person to guess the answers to. However, it can be difficult to design these questions. In this activity, you'll try and guess the answers to recovery questions for celebrities' accounts. How many can you find by searching online?

Xherdan Shaqiri
What is your mother's maiden name?
What is your favourite colour?
What city were you born in?
What was your first phone number?
What is your favourite sport?

Justin Bieber
What is your mother's maiden name?
What is your favourite colour?
What city were you born in?
What was your first phone number?
What is your favourite sports team?

Ariana Grande
What is your mother's maiden name?
What is your favourite colour?
What city were you born in?
What was your first phone number?
What is your favourite book?

Rihanna
What is your mother's maiden name?
What is your favourite colour?
What city were you born in?
What was your first phone number?
What is your favourite actress?

Roger Federer
What is your mother's maiden name?
What is your favourite colour?
What city were you born in?
What was your first phone number?
What is your first child's name?

Supplemental materials to accompany Stobert, E., Cavar, E., Malisa, L. and Sommer, D. (2017) Teaching Authentication in High Schools: Challenges and Lessons Learned. 2017 USENIX Workshop on Advances in Security Education.

Which of these questions do you think is the most secure? Why?

Which of these questions is the least secure? Why?

Is it a good idea to use personal information for authentication? Why or why not?

If a friend tried to access an account of yours using the personal knowledge questions, would they be able to use Google to find the answers? What other information might they have available that could help them answer these kinds of questions?

Are personal knowledge questions the only way to reset a forgotten password? What is another method that could be better? Why?

In this activity, you've guessed personal information to gain access to an account through the password reset mechanism. Based on what you've found here, is it a good idea to include personal information in passwords? Why or why not?

Graphical Passwords

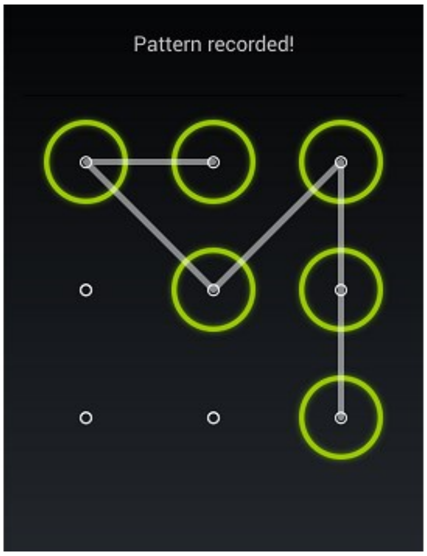
Although most of the passwords we encounter regularly are text passwords, there are other types of passwords. Graphical passwords are passwords that use pictures. There are many different types of graphical passwords that work different ways and use pictures in different ways to help users log in more easily.

In this activity, you will try out different kinds of graphical passwords to see how they work and how memorable you find them.

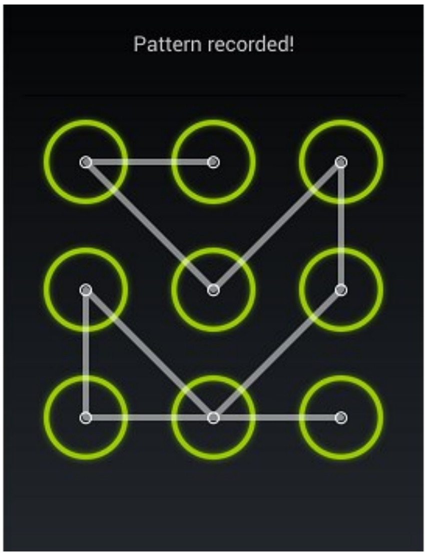
Android pattern lock (use on Android phone)

The Android Pattern Lock is a graphical password on Android phones that can be enabled to lock the screen. In this system, the password consists of a small drawing on a grid. To log in, the user has to recreate the drawing (touching the same grid squares in the same order).

On the Android phone, go to the app drawer, then the Settings menu. Scroll down and choose the Security menu, then choose Screen Lock and set it to Pattern. Choose and confirm a pattern password and then use it to unlock the phone. Be careful not to forget the password!

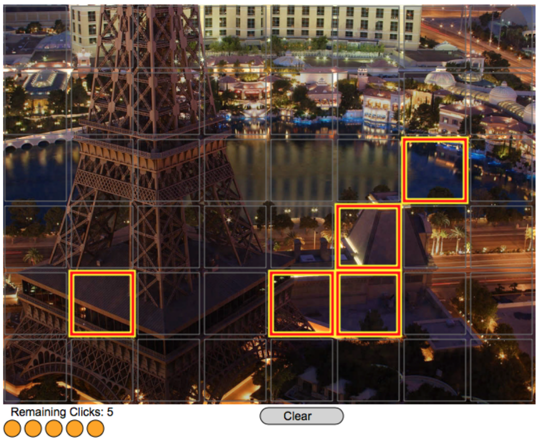


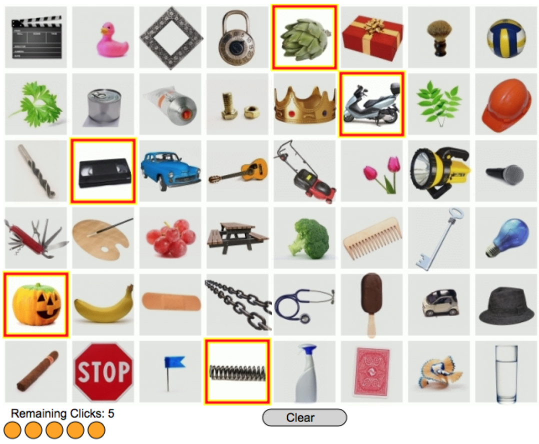
Pattern recorded!

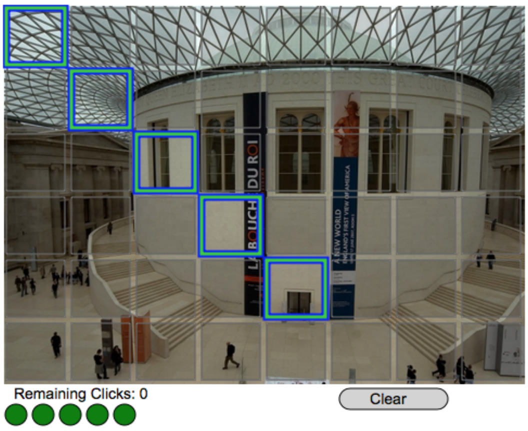


Pattern recorded!

PassTiles (assigned, user chosen, objects)







PassTiles is a graphical password system where the password consists of a set of squares (tiles) on a grid. To log in, the user has to click on the five password tiles that are part of their password. The order that the user clicks the tiles does not matter.

There are three different variations of PassTiles:
a) In Image PassTiles, the system assigns five password tiles to the user. The user must remember the tiles based on their grid position and the part of the image that is underneath each tile. The order does not matter.

b) Chosen PassTiles works exactly like Image PassTiles, but the user gets to choose their own password instead of having it assigned by the system.

c) In Object PassTiles, the system assigns five object images to the user. To log in, the user has to click on the correct objects, which will appear in different positions on the grid at every login.

Go to: *Link available upon request*

Choose a username. Be sure to try all three systems (IPA, IPU, and OPA usernames).

Type in the username, then press Create to begin. Follow the instructions to create, practice, and confirm your password. If you need help, follow the link.

Image PassTiles	Chosen PassTiles	Object PassTiles
IPA_1	IPU_1	OPA_1
IPA_2	IPU_2	OPA_2
IPA_3	IPU_3	OPA_3

How do you find that these passwords compare to text passwords? Do you think you'd be able to remember your graphical passwords if you used them in real life?

If you watched a friend log in using these types of system, would it be easier or harder than with text passwords to figure out their password?

For the Android Pattern Unlock, do you think that you could figure out another user's password pattern by looking at the screen of their phone?

Try doing this: have your friend unlock the phone several times (without showing you), and then try to figure out their unlock pattern. If you mess it up, have them redo the "smudge marks" on the glass. Can you get it right?

Was it easier or harder to remember the object images or the background images? Which do you think would make a better password?

When you and your group members chose your own PassTiles passwords, did you choose any of the same squares? Why is it safer to assign these types of passwords?

How many possible passwords are there for (unordered) PassTiles passwords? Explain how you calculated it.

Do you think that these passwords are more or less secure than text passwords? Why?

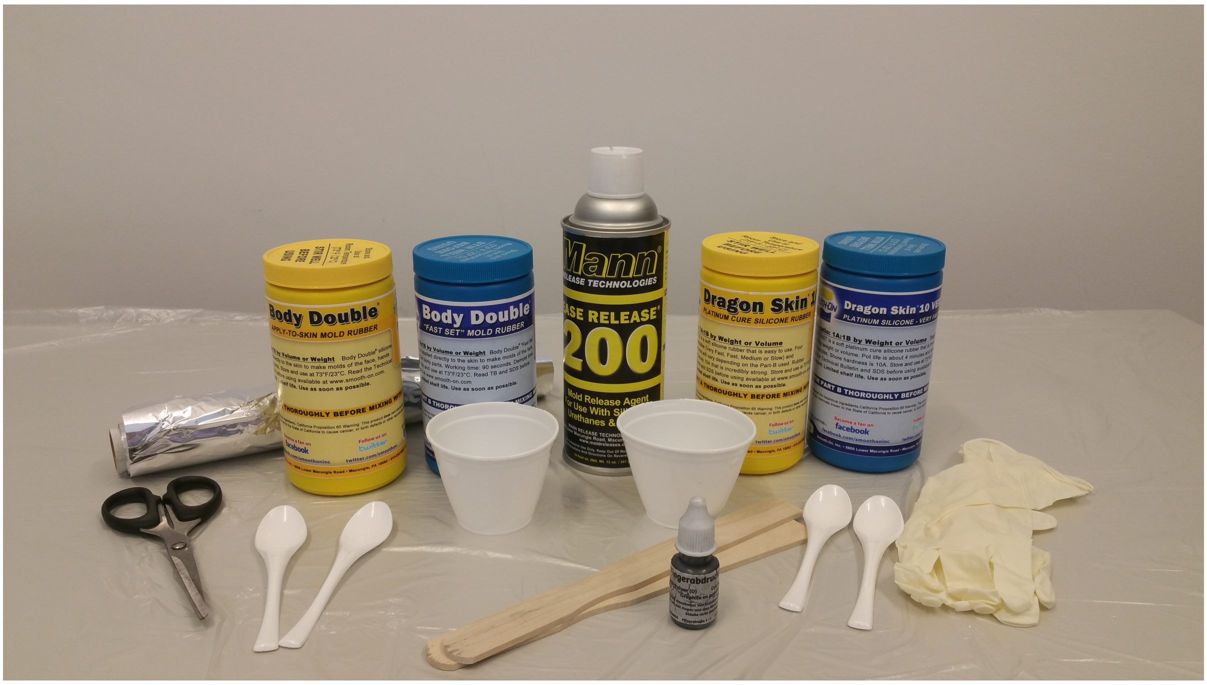
Biometric Authentication

Another way of authenticating is by checking a unique property of the person trying to authenticate. These unique properties of bodies are called *biometrics.* The most common biometric used for authentication is the fingerprint, but scans of the iris, the shape of the ear, and the pattern of veins in the hand can all be used to uniquely identify someone.

In the first part of the activity, you will make a copy of your finger, and try to use it to unlock your phone. If you don't have a phone with a fingerprint scanner, you can try it on one of the demonstration phones.

In the second part of the activity, you'll learn about how fingerprints can be lifted from everyday surfaces.

Materials

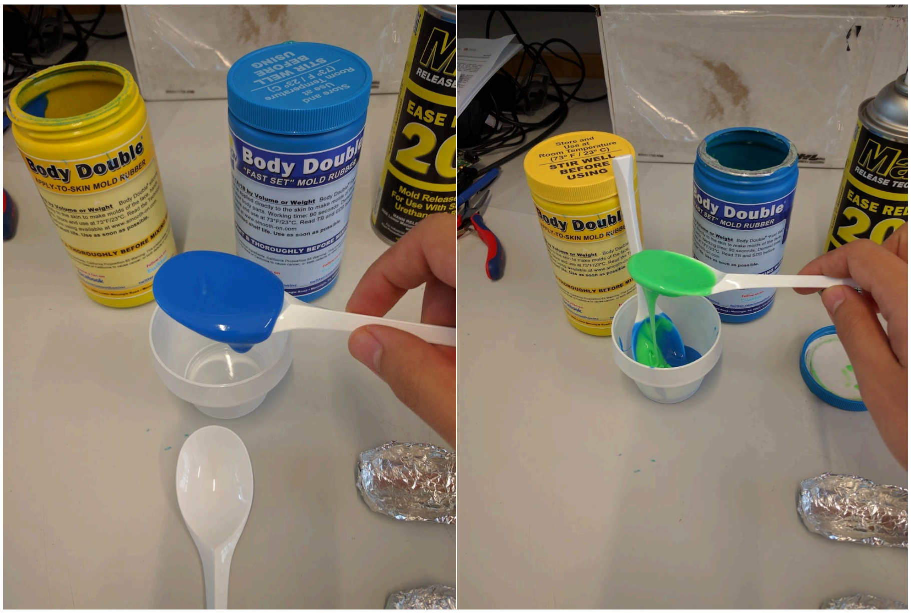


Here is a list of all the materials that you will need. On the left side, you see the material for making the mold ("Body Double"), a plastic cup and two large spoons for mixing the mold. In the middle you see two aluminum foil "cups" that you will use to pour the mold and cast into. On the right side you see the silicon ("Dragon Skin") for making the cast, as well as a separate mixing cup and two smaller plastic spoons. You will need to make the aluminum foil cups.

You should remove any jewellery from your hands (rings, bracelets) before beginning this. The materials can be messy, so if you brought an old tshirt or an apron, put it on now.

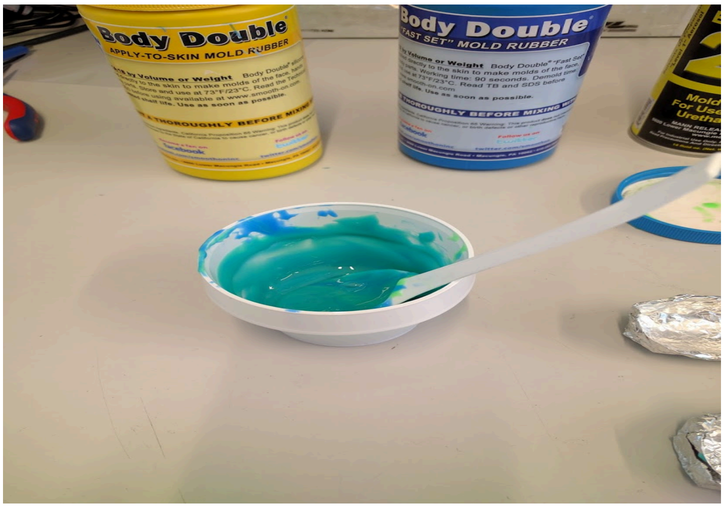
Supplemental materials to accompany Stobert, E., Cavar, E., Malisa, L. and Sommer, D. (2017) Teaching Authentication in High Schools: Challenges and Lessons Learned. 2017 USENIX Workshop on Advances in Security Education.

Step 1



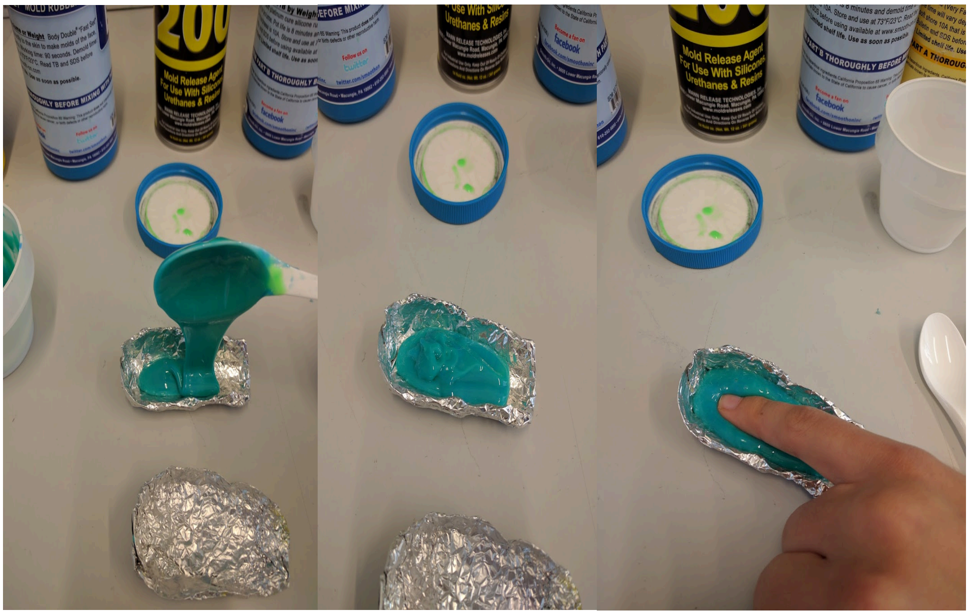
Take a plastic cup and two clean **BIG plastic spoons**. Using separate spoons, take one spoonful of the **blue** Body Double (component A)**,** and one spoonful of the **green** Body Double (component B) and put them in the plastic cup.

NOTE: Don’t use the same spoon for both components. Be sure that you take each component with a new, clean spoon.



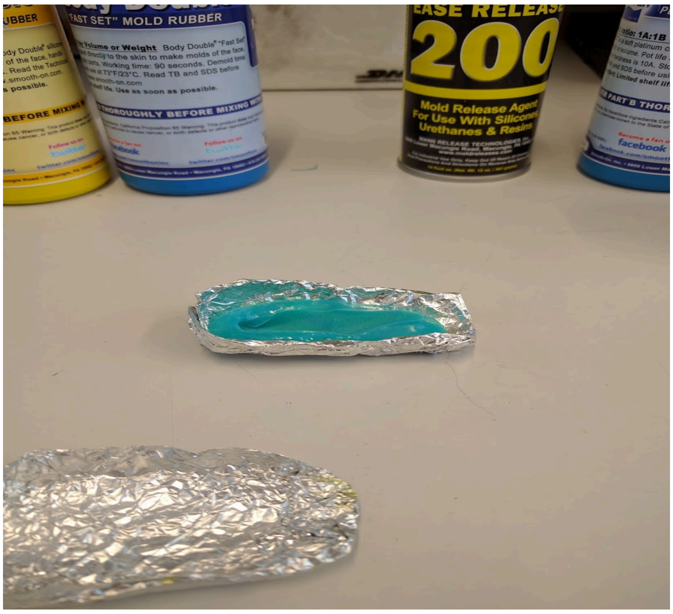
Mix the two components until you see only one colour, turquoise. Try to avoid creating air bubbles as you mix. This is how the substance will look when you mix it well.

Step 2



Using the large spoon, take a spoonful of the mixed substance, and pour it in the aluminum foil. Then place the finger that you use to open your phone in the substance. Don't press too hard, and keep the finger still for 7-8 minutes.

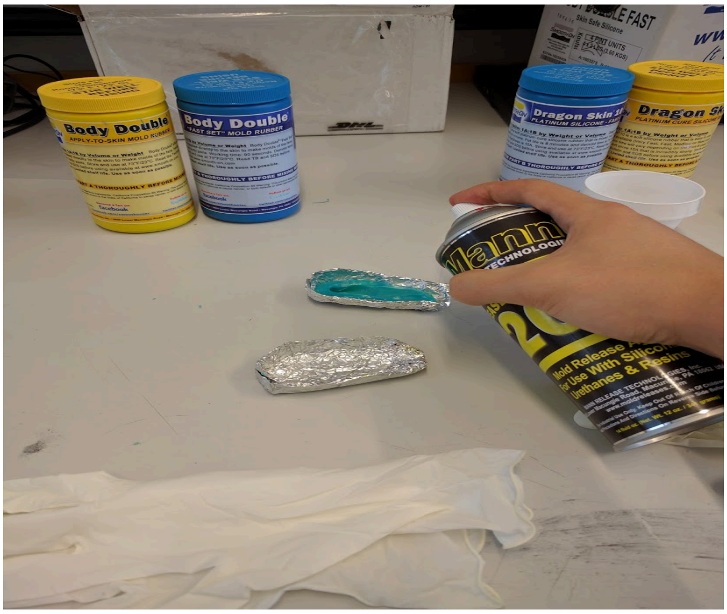
Step 3



Gently remove your finger from the mold.

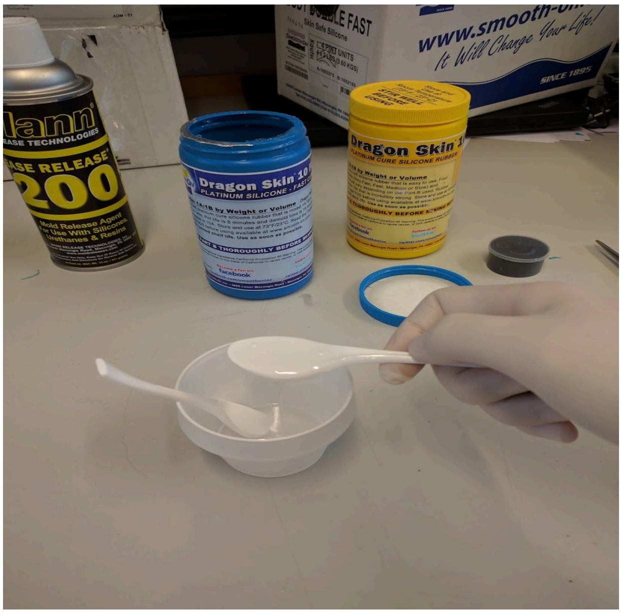
Supplemental materials to accompany Stobert, E., Cavar, E., Malisa, L. and Sommer, D. (2017) Teaching Authentication in High Schools: Challenges and Lessons Learned. 2017 USENIX Workshop on Advances in Security Education.

Step 4



To make sure your finger mold and the silicon will be able to separate later on, take the **Ease Release** spray, and spray the inside of the mold twice, for one second each time. Make sure that you spray the interior of the mold well, otherwise the silicon won't separate from the finger cast.

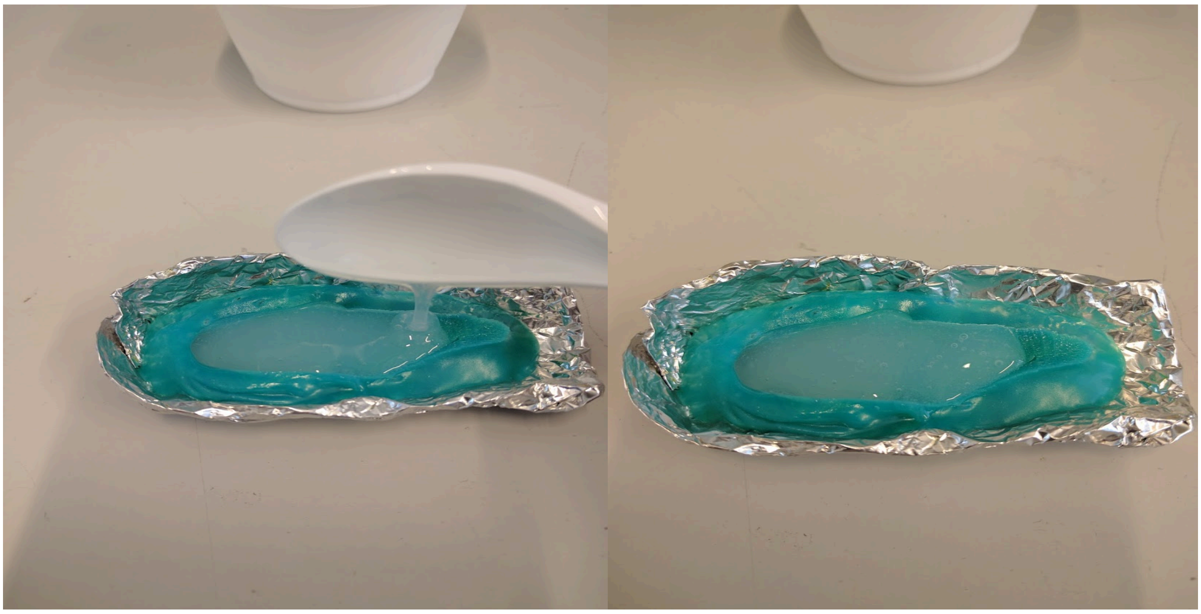
Step 5



For the next step, you will be mixing two new components of **Dragon Skin** to make silicon. Put on your **gloves** now, as the silicon is sticky. Take a **clean plastic cup** and **two small plastic spoons.** Using two spoons, take one spoonful of each component (both components are white), put them in the plastic cup and mix well. You will use these components to make a cast from your finger mold.

NOTE: Don't use the same spoons on both components. Be sure that you take each component with a new, clean spoon.

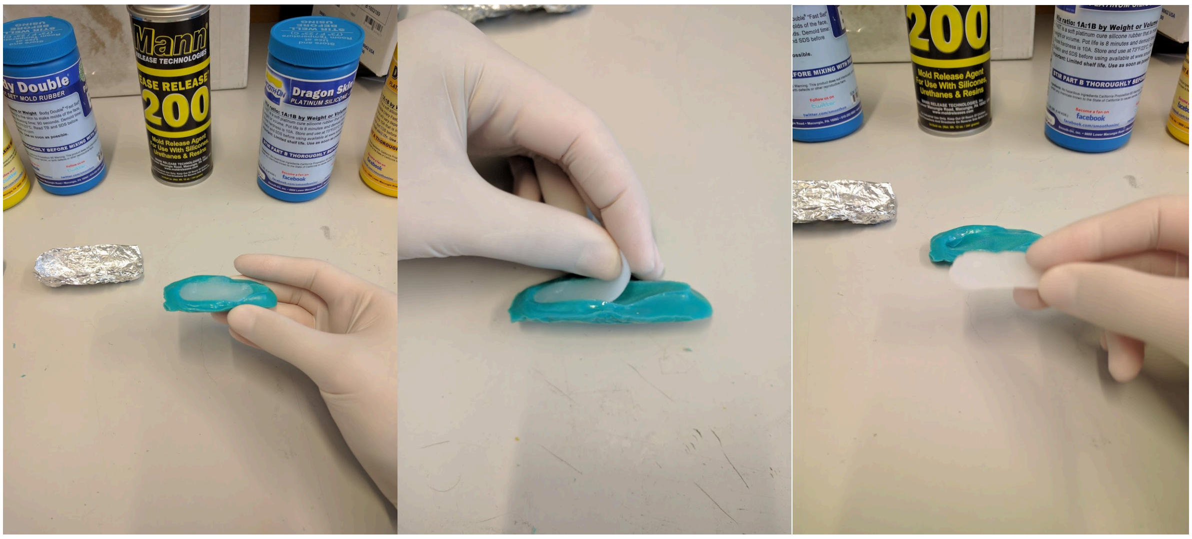
Step 6



Once you have mixed the two components well, take one spoonful and gently pour it over the mold you've made in the previous steps. If you see air bubbles, tap the mold gently to encourage them to rise. Set the mold on a piece of paper and **label it with your name.** Leave the silicon to dry.

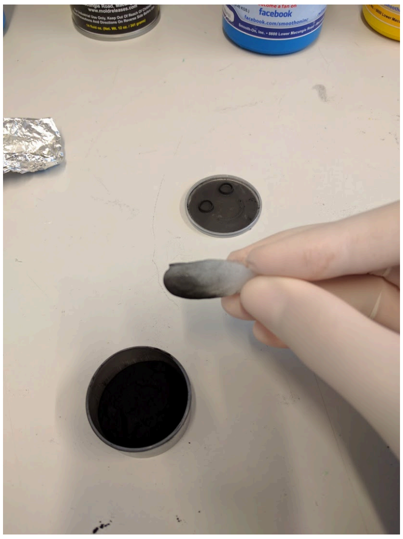
Step 7

Now that the silicon has had time to harden, you can unwrap your finger and use it to try and unlock your phone.



When the silicon has hardened, gently remove the silicon cast from the mold. You have made a copy of your finger in silicon!

Step 8



We cannot use the silicon finger to unlock the phone just yet. The phone fingerprint sensors detect conductivity, and our silicon finger is not conductive. Take the silicon finger and dip it gently into a fine graphite powder. Then gently spread the graphite around the finger, using a cotton swab.

Now try unlocking the phone. Does it work?

When you finish this activity, you can keep the copy of your finger, but you should make sure to damage the fingerprint so that it can't be stolen and used to unlock your phone. Take a pair of scissors and make a little cut out of the fingerprint when you finish the activity.

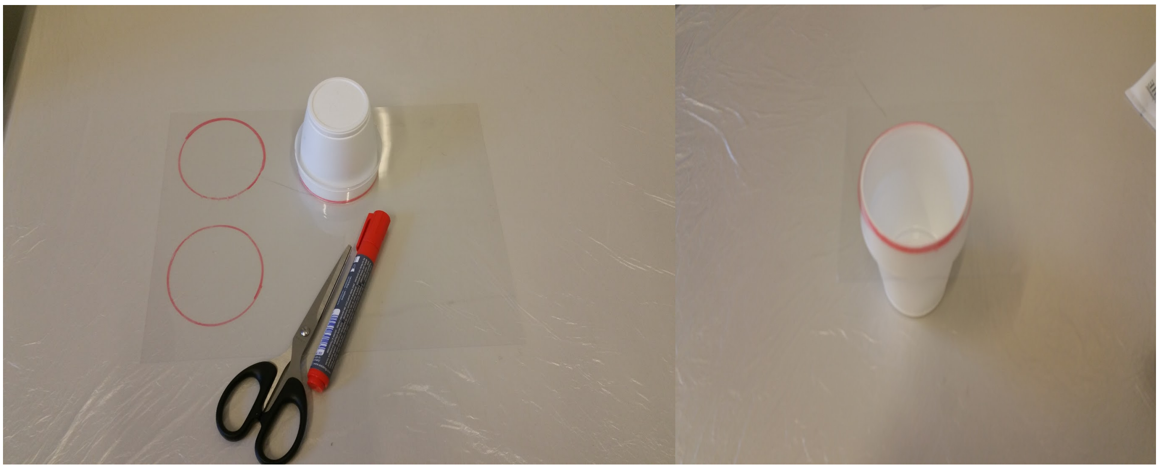
Activity 2

Fingerprint authentication is convenient and fun to use, but our fingerprints are not as secret as they may seem. In this activity you'll learn how imprints of our finger ridges are left on many surfaces as we handle them in everyday life.

In this activity, you will use a simple method for lifting fingerprints. This is the first step that an attacker would need to take if they were trying to access an account that had a fingerprint reader.

Step 1

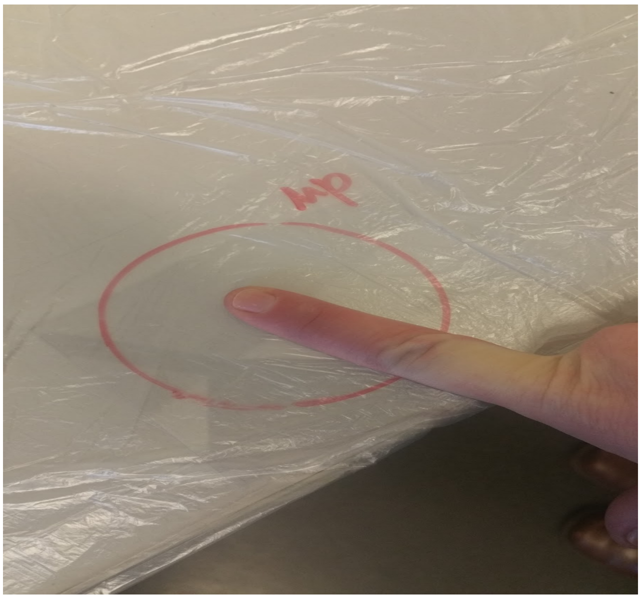
The best quality fingerprints are lifted from a smooth hard surface, so we will use a plastic transparency.



Start by placing the cups on the transparencies, and tracing a circle around the cup. Proceed by cutting the transparencies into squares so that they fit neatly over the plastic cups, covering the whole top of the cup.

Make sure you have: (i) the cup, (ii) the transparency, and (iii) super glue ready.

Step 2



Take your finger and rub it on your forehead, so that the finger has sufficient grease on it to make a nice print. Then place the finger in the middle of the red circle on the transparency (create a fingerprint). Press your finger down neatly once in the circle, and don't smudge it around or redo it.

Step 3

Open the super glue, and pour a little bit onto the bottom of the cup. Then take the transparency with your fingerprint, and place it over the cup.

NOTE: Make sure that the side of the transparency with your fingerprint is facing DOWN (towards the glue).

Supplemental materials to accompany Stobert, E., Cavar, E., Malisa, L. and Sommer, D. (2017) Teaching Authentication in High Schools: Challenges and Lessons Learned. 2017 USENIX Workshop on Advances in Security Education.

Leave the fingerprint for 5 - 10 minutes so that the glue can evaporate and make your fingerprint more visible. Leaving it in a warm place will speed up the process.

Step 4

Congratulations! You should now have a nicely visible and fixated fingerprint!

Were you able to unlock your phone using the fake finger? If not, what do you think went wrong?

What are three advantages of using biometrics for authentication?

In a system that used fingerprints for authentication, how could you change your "password"? Do you have an unlimited number of password changes?

Can you think of any privacy problems related to using fingerprints for authentication? Would it be a good idea to use fingerprints for authentication on a system where you wanted your identity to remain secret?

Based on this activity, do you think it's a good idea to use fingerprints for unlocking a phone? Do you think it would be a good idea to use fingerprints for authentication on a high-security system such as a bank account?