Teaching Authentication as a Life Skill

Elizabeth Stobert, Elizabeta Cavar, Luka Malisa, and David Sommer | ETH Zurich

As more and more of the activities of daily living move into the digital realm, the importance of securing those activities grows. Where once an understanding of password security might have been considered a useful bonus, it is now becoming an integral life skill. Users of all ages need to be aware of what information is shared online and how to secure it. It is crucially important that security be taught at an early age, before users are faced with the full magnitude of security management tasks. In this article, we present our work developing security curriculum modules for teenagers, and discuss our attempt to teach life skills for security to Swiss high schoolers.

We chose to focus first on the skills associated with user authentication. Authentication tasks are pervasive—almost every interaction with a web service involves creating a username and password, making the impact of good password practices significant. In addition, users’ authentication problems are relatively well-researched and well-understood, providing us with clear ideas for what kind of interventions are needed. Authentication is far from the only skill users need to secure themselves online, but for our purposes it seemed like a natural starting point. Users often have poor mental models for security,¹ and lack a framework for reasoning about the threats affecting passwords and security.² Although users do try to invest greater effort into more important accounts, they often do not understand how to effectively create stronger passwords.

The goal of our curriculum was to educate about authentication, specifically patching the gaps that have been uncovered in research on adult users’ understanding of passwords and password management. Considering long-term goals, we wanted to plant ideas that could support good authentication habits through a lifetime of changing services and technologies.

Authentication Activities
We designed five activity units, each focusing on a different aspect of authentication. Each activity was independent of the others and designed to be completed in groups of two to four students. For each activity, we developed an accompanying worksheet to guide students through the activity and support their learning with directed questions. Further information on the activities below can be found in our extended paper.³

Creating Strong Passwords
The goal of this activity was to have students think critically about what features have the greatest impact on the creation of strong passwords. We used the Dashlane password security estimator (www.howsecureismypassword.net) to provide direct feedback about the impact of different password characteristics on password guessability (using estimated guessing time as a metric for strength against attack). In the activity, we had students explore different password policies and experiment to find the weakest and strongest passwords that could be created under those policies. The Dashlane security estimator tool also factors in features such as word popularity to its guessing time estimates, and we used this feature to have students experiment with different password features and connect them with guessability. We drew students’ attention to dictionary words, common date patterns, keyboard patterns, and the fallibility of assuming that other languages will provide secure passwords. In this activity, we avoided teaching prescriptive rules about password creation and tried to emphasize the idea that a variety of factors can affect password strength.

Password Cracking
To help students understand the types of nontargeted threats that affect passwords, we designed an activity to introduce students to strategies that might be used in password guessing attacks. We created a scenario where students were “hackers,” trying to guess bank passwords. We told them they had gained access to a list of disguised (hashed) bank passwords, and that they had to try to guess the passwords that corresponded to the provided hashes. We created a list of 20 passwords for students to guess. Using an accompanying website tool that allowed students to check their guesses, students were encouraged to guess as many plaintext passwords as possible. To minimize confusion, plaintext passwords were numerical and the hashed passwords were entirely alphabetic. The list of hashed passwords was designed to reward students for using guessing strategies that reflect actual techniques used in password attacks. We seeded the
list with passwords that could be easily guessed using dictionary or brute-force guessing strategies and, in the worksheets, explicitly defined these concepts and asked students to apply them. The worksheet also asked students to consider defenses against guessing attacks such as lockout policies and randomly assigned passwords, and their attendant advantages and disadvantages.

**Graphical Passwords**

Although the majority of authentication events use passwords, text passwords are not the only form of authentication. To introduce the concept that authentication does not necessarily mean passwords, we designed an activity about graphical passwords, or passwords that use images for login. In this activity, we introduced the Android pattern unlock mechanism, and also PassTiles, a graphical password system used in research.

Students created passwords in both systems and tested their memory for these passwords. PassTiles is designed to make system-assigned passwords memorable, and we asked students to evaluate the memorability of these passwords (see Figure 1). Our goal in this activity was to encourage students to think critically about how risks change in different systems and to use novel password systems to help them question their assumptions surrounding text passwords. We asked students to consider the security of these types of passwords compared with text passwords, and to explain their logic. We also introduced the concept of shoulder-surfing attacks and contrasted this risk with guessability.

**Personal Knowledge Questions**

Targeted threats also affect users, and in this activity, we focused on how personal information can be leveraged to breach accounts. Using a password recovery scenario, we created fake personal knowledge questions (and answers) for five celebrities. We framed the students as attackers attempting to gain access to the system and told them to see how many of the questions they could answer using a web search. We selected questions that highlighted different problems with personal knowledge questions, including questions with limited answer sets, questions with answers that are easily searched, and questions with unmemorable answers.

In the worksheet, we asked students to consider what kind of personal information is easily available to friends or acquaintances and why it is not a good idea to include personal information in authentication. We further explored the topic of recovery authentication and asked students about what kinds of alternative systems might be more secure. Finally, we connected the dangers of including personal information in recovery authentication to passwords and other forms of authentication.

**Biometric Authentication**

Biometric authentication is increasingly deployed on consumer devices and is popular with users. Fingerprints are one of the most well-known forms of biometric authentication and are conceptually familiar from long-term use in forensic crime solving.

In recent years, fingerprint readers have become widely deployed on mobile phones and used for device authentication. Users are often extremely enthusiastic about biometric authentication, believing it to be more secure than passwords. In this activity, we explored the security advantages and risks of biometric authentication. In this activity, we demonstrated that fingerprints can be easily spoofed. Students used commercial modeling silicone to create copies of their own fingerprints, which when dusted with graphite powder, would fool the fingerprint reader and unlock their smartphone (see Figure 2).

Inconsistency in student modeling technique meant that only some students were actually successful in unlocking their phones, but all models were sufficiently detailed to convey the concept of the attack. For simplicity and accuracy, we had students lift their fingerprints directly from their fingers, but we also included a small demonstration of how easily fingerprints can be lifted from other surfaces using superglue to “illuminate” fingerprints left on acetate transparencies. In the worksheets, we used the silicone models to draw students’ attention to the idea that biometric information is not necessarily as secret as is often assumed. We also
discussed the privacy issues attendant to unique and unchangeable identifiers and linked this to the difficulties of credential revocation with biometrics.

**Pilot-Testing**

We pilot-tested these materials as part of outreach workshops in four high school classrooms around Zurich, Switzerland, between October 2016 and January 2017. Students in the workshops ranged from 14 to 18 years old. Although the activities do not require an expert instructor, we conducted the workshops ourselves so that we could better understand how the activities functioned in the classroom. We began each workshop with a presentation on the basics of authentication: what authentication means and why it is necessary, how we authenticate in the real world, and the difference between identifiers and secrets in the authentication process. We also briefly discussed the ethics of studying security and emphasized that knowledge of attacks does not make it acceptable to try them on friends or family.

Each activity was designed to take approximately 30 minutes. When testing these activities in the classroom, we used a round-robin format where the class was broken into small groups, and those groups rotated through the activities. This forced the class to stay on approximately the same schedule, avoiding stragglers. The biometric activity was longer than the others and required a delay while the silicone cured. To accommodate this, we broke the activity into two parts: an initial session where the models were created, and a second part where the completed models were tested on phones and the students completed the worksheets.

The activities cover various aspects of authentication and are designed so that they can be used together, but they may also be used separately. In different pilot tests, we used various subsets of the activities and, in one short test, used only the biometric activity. The worksheets can also be supplemented for additional enrichment. In one workshop, we asked each group to make a poster about one activity and, at the end of the day, present that poster and answer questions from their peers about the authentication topic.

The activities were designed to encourage engagement and interaction with the concepts underlying authentication. The worksheets were accordingly designed to encourage students to think about the advantages and disadvantages of different types of authentication and to consider why there may not be a single right way to authenticate. Accordingly, the worksheets were not designed to have single correct responses. In our workshops, we ended the day with a group discussion of the worksheets, highlighting the issues we wished to see covered, and hearing students’ findings on the topics.

**Discussion**

In our materials, we wished to strike a balance between providing practical guidelines and teaching about the theoretical underpinnings of computer security. We wanted to focus on practical, actionable advice but did not want to reduce our curriculum to unsupported heuristics that would not help users reason about security. We anticipate that teenagers will be asked to create increasing numbers of passwords and make other authentication-related decisions as they grow into adulthood, and part of our goal was to ensure that the materials we provided for them would scale with and support this growth. However, we also wanted to provide sufficiently straightforward guidelines that all students could immediately apply to their current authentication tasks.

In designing our activities, we tried to take into account the natural constraints of both students and teachers in a typical high school. A general audience of high school students is unlikely to have a preexisting interest in computer security. Depending on their grade level and the high school curriculum, they may also have limited knowledge of general computer science topics and be unable to strongly engage with the technical concepts underlying security concepts. Similarly, the availability of teacher knowledge and resources might be limited. To reduce barriers to classroom implementation, we attempted to design self-contained, student-led modules.

Security skills have never been so necessary to end users and, given current trends, will only continue to increase in importance. All users need to be able to make informed decisions about protecting their accounts and securing their data. Approaching security education from the perspective of teaching life skills gives a useful framing for deciding what to teach, when to teach it, and how to design the lessons. We know that the objectives outlined here will be familiar to educators and researchers working in this area. Our efforts are far from the last word on the topic, but we hope that these activities and our experiences pilot-testing them in high school classrooms will contribute to the broader efforts to help young users secure their data. It is easy to assume that computer security is not necessarily of interest to many teenagers, but in the right context, security and privacy issues matter deeply to teenagers.

There is a distressing tendency for both security professionals and many users to consider the state of being secure as all-or-nothing, and tenets like the “barn door principle”
support that. Most singular security tasks are manageable, but when faced with tasks like creating strong passwords for all of their accounts, users tend to be overwhelmed. But when reframed as a life skill, it becomes clear that every little bit helps. There are few guarantees to be made, but we think that it is incredibly important to emphasize to teenagers (and other users) the idea that they do not have to solve the entire security problem in order to ameliorate their personal situation.

All of our activities and supplementary materials, including the introductory presentation, are available for download in both English and German at www.syssec.ethz.ch/research/high-school-security-education.html.

References

Elizabeth Stobert is a postdoctoral fellow at Concordia University in Montreal, Canada. At the time of this work, she was a postdoctoral researcher in the Systems Security group at ETH Zurich. Contact at elizabeth@stobert.ca.

Elizabeta Cavar is a Specialist (Expert) in the group Information Technology and Education, Department of Computer Science at ETH Zurich. Contact at elizabeta.cavar@inf.ethz.ch.

Luka Malisa is a postdoctoral researcher at ETH Zurich. Contact at luka.malisa@inf.ethz.ch.

David Sommer is a PhD student at ETH Zurich. Contact at david.sommer@inf.ethz.ch.

IEEE Computer Graphics and Applications bridges the theory and practice of computer graphics. Subscribe to CG&A and
• stay current on the latest tools and applications and gain invaluable practical and research knowledge,
• discover cutting-edge applications and learn more about the latest techniques, and
• benefit from CG&A’s active and connected editorial board.