Teaching Authentication in High Schools: Challenges and Lessons Learned

Elizabeth Stobert, Elizabeta Cavar, Luka Malisa, David Sommer
ETH Zurich
first.last@inf.ethz.ch

Abstract

As more of the activities of daily living take place online, computer security education for high school students is of increasing importance. To address this need, we designed, developed, and tested prototype curriculum materials to teach secondary school students about user authentication. We identify challenges encountered in this process, and contend that these challenges stem from the nature of security and are inherent to teaching it. We suggest that other safety-related topics (such as sex education) could provide valuable parallels for designing computer security curriculum.

1 Introduction

Educating teenagers about computer security is of utmost importance. Increasing quantities of personal information and data are stored online, and many aspects of social interaction have shifted into an online sphere. The choices that teens make around computer security may have profound and long-lasting consequences for the protection of this information. Authentication is a computer security task that is omnipresent for end users, and where educational efforts are needed to help users adequately protect their accounts and data.

In this paper, we present our experiences developing curriculum materials to teach Swiss high school students about user authentication. We describe our prototype curriculum, and identify a number of challenges that we encountered while designing, developing, and testing our prototype materials. We contend that many of these challenges stem directly from the properties of security, and are inherent to teaching security. We expect that these challenges will be familiar to those who have worked in this area, but we hope that there is space to begin a discussion about how these challenges relate directly to what we are trying to teach, and to address such issues in the greater context. We suggest that in the context of secondary school education, computer security should be approached from the perspective of other health and safety-related topics, such as sex education.

2 Background

Authentication is the primary security task affecting end users. Passwords are notoriously unusable, and their design creates tensions between the capabilities of the human brain and strong security properties. The "password problem" [17] is that the passwords that are easy for users to remember are also easy for attackers to guess. Essentially, passwords must be designed so that the same task (accessing a system) is easy for the legitimate user, but impossible for the illegitimate user (the attacker).

The long-time narrative of the "lazy user" suggests that if users were willing to work harder, security problems with passwords could be solved. However, a cost-benefit analysis of managing passwords [6] shows that users could invest substantial amounts of time into password management without reaping significant security benefits, and that users are behaving sensibly they mitigate the demands of passwords by using coping strategies such as reusing passwords. Research examining how users cope with passwords finds that users manage passwords by devoting additional effort to accounts of increased importance, and minimizing attention paid to less important accounts [13].

However problematic passwords are for both users and security, they are an embedded technology that is unlikely to be replaced [7]. Passwords have a number of advantages: they are cheap, easily implemented, easily revoked, and comprehensible to users. Moreover, they are the status quo, and from the perspective of education, an important area in which small improvements might result in widespread advantages for users. Although the design problems with passwords will not be solved by education, there are a number of ways in which users' coping strategies could be strengthened by better understanding of the risks and threats surrounding passwords.

2.1 Children and Authentication

Security considerations for children have different constraints than those of adults. Zhang-Kennedy et al. [18] found that childrens' (aged 7 to 11) perceptions of mobile privacy concerns were significantly different from their parents, and that parents were taking an active role in protecting their children from privacy threats online.

Research examining childrens' password knowledge finds that children have some basic understanding of what password characteristics contribute positively to security [3]. But children may not have a strong understanding that passwords are meant to be secret, and must not be shared [10]. Read & Cassidy found evidence that children understand the concept of a password, but are tripped up by design characteristics such as spelling and length [10]. Assal et al. [1] examined the memorability of graphical passwords with children and adults and found that while both preferred the graphical passwords, the children were more likely to have difficulty committing the passwords to memory.

Less work has examined the security habits of teenagers. Boyd [2] explored the role of social media in the lives of American teenagers and found that it has become integral to teenagers' social lives, but that the affordances of social media (persistence, searchability) create new social dynamics that have associated security and privacy concerns. Educational efforts directed at teenagers need to acknowledge these realities.

3 User Authentication Curriculum

As part of an effort to consider how computer security education might be integrated into future Swiss secondary school curricula, our research group was asked to consider what topics might be of importance to cover in high schools and to develop prototype teaching materials. Although outside the scope of this paper, we sketched curriculum guidelines for five topics in computer security, and in the first phase of the project, developed a detailed prototype of teaching materials (including activities and worksheets) for the module on user authentication.

We chose to first focus on authentication because it is one of the largest security tasks affecting end users of all ages. Proving that someone is who they say they are is one of the cornerstones of security, and when users think about security, they often consider passwords as the central security task that affects them. Most users keep track of large numbers of accounts (estimates typically fall around 25 accounts [4]). As well as authenticating to websites, users must also authenticate to mobile devices and other computers. Users authenticate many times per day [11], and are asked to create and remember large numbers of passwords [5].

3.1 Design Goals

In designing our curriculum, we had a number of goals.

The first goal of our curriculum was to educate about authentication, specifically addressing gaps in adult users' understanding of passwords and password managements. Users often have poor understanding of the threats affecting passwords, and lack a framework for reasoning about passwords and security [13]. Although users do try to invest greater effort into more important accounts, they often do not understand how to effectively create stronger passwords. Considering long term goals, we wanted to plant ideas that could support good authentication habits through changing accounts and technologies.

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 other authentication-related decisions as they grow into adulthood, and part of our goal was that the materials we provide for them should scale with and support this growth. However, at the same time, we wanted to provide sufficiently straightforward guidelines that all students could immediately apply them to their current authentication tasks.

Much of the research in security education is aimed at university undergraduates. This user group has significant differences from the secondary school students who formed our audience. Our students had no pre-existing interest in computer science, and had varying educational backgrounds. In Switzerland, students specialize at the high school level (around age 12), and are streamed into one of either an apprenticeship program "Berufsschule", general-admission secondary school "Sekundarschule", and limited-admission secondary school "Gymnasium" (pronounced with a hard G, as in gum)[1]. In addition to this, different gymnasiums specialize in different topics, and students are streamed into specialty programs where they may have additional emphasis on topics such as music or sciences. This meant that students in our audience could vary significantly in educational level, particularly in mathematics.

[1] More detail about the Swiss education system, and how it varies by canton can be found here: `http://www.edudoc.ch/static/web/bildungssystem/grafik_bildung_d.pdf`

Another consideration in the design of our curriculum material was the availability of teacher knowledge and resources. We endeavoured to design materials that could be integrated into classrooms without requiring teachers to develop expertise on the topic. We think it is important to reduce barriers to classroom implementation, and that creating self-sufficient materials should encourage teachers to try the activities in their classrooms. Toward this goal, we attempted to design each activity as student-led inquiries, with complete instruction sets that should not require strong teacher guidance.

3.2 User Authentication Curriculum

We structured our prototype authentication module as a set of five activities. Each activity was designed to take about 30 – 45 minutes, and to be worked on in groups of 2 – 4 students. The intention was that in order to keep students on a steady schedule, the activities should be worked by small groups of students in a round robin. The activity rotation was bookended by an introductory presentation about the principles of authentication, and an interactive discussion about the results of each activity[2].

To the best of our ability, we designed our curriculum materials so that they involved active experimentation and hands-on interaction with the principles of security that we were trying to teach. As a technical subject, security can be considered dull, and we felt it was important to design materials that engaged students and related the material to their own contexts as much as possible. As well, we were cautious about appearing prescriptive or "bossy", and wanted to present the material as a structured inquiry for students, rather than as a set of dictums for safe behaviour.

In our materials, we covered a variety of topics relating to passwords, and good password practices. For our introduction, we created a presentation that explained the concept of authentication and shared secrets. Using a structured discussion, we introduced the three types of authentication (something the user is, has, or knows), and led students through thinking about where, how, and why we authenticate in real life.

3.2.1 Creating Good Passwords

This activity was designed to have students explore the question "what makes a good password?" Using estimated guessing time as a representation of strength against guessing attack, the activity encouraged students to experiment with different password features and to understand how those features impact guessing time. In the worksheet questions and discussions, we asked students to connect password features with their guessability, and to connect these features to how passwords might be easily guessed. We drew attention to dictionary words, prominent dates, keyboard patterns, and the fallability of assuming that other languages will provide secure passwords. One of the problems with password creation (and indeed, even many password meters [15, 14]) is that little feedback is given about how different password characteristics affect security.

We used the Dashlane password security estimator (`www.howsecureismypassword.net`) in our activity. This tool gives a time estimate for how long entered password strings might take to be guessed, and provides feedback on the password characteristics that affect the strings' guessability. Important for us was that the tool integrates features of both brute force and dictionary attack in creating its estimates. Students were explicitly warned not to try their real passwords in the tool.

3.2.2 Cracking Passwords

This activity was designed to introduce students to the concept of guessing attacks, and to help students think about the different tactics that attackers might use when approaching the task of password guessing. Indirectly, the activity was also intended to address users' frequent misconception that all guessing attacks are personal, and targeted at a particular user. Through a role-playing scenario where students pretended to be attackers guessing passwords on an offline list, we hoped to communicate the concept of "impersonal" attacks.

In this activity, we created a scenario where students were "hackers", trying to guess bank passwords to steal money from a local bank. We told them they had gained access to a list of disguised (hashed) bank passwords, and that they had to try and guess the plaintext passwords that corresponded to the provided ciphertexts. To clarify the distinction between the plaintext and ciphertext, we design the activity so that all plaintext passwords were PINs (i.e., 4-digit numeric strings) and that all encrypted passwords were 4-character alphabetic strings. We told students that they knew the bank's method for disguising passwords, and we wrote a small tool that allowed students to check their guesses. We provided a list of 20 passwords for students to guess, and seeded the list with passwords that could be obviously guessed using dictionary or bruteforce guessing strategies. In the worksheets, we drew students' attention to these particular guessing strategies, and encouraged them to explore how such strategies could help their own guessing. We also motivated the concept of a lockout policy by asking students why repeated guessing would not work on their regular accounts.

[2] Our activity materials and worksheets can be downloaded on the ASE 2017 workshop website.

3.2.3 Graphical Passwords

To explore the idea that passwords do not necessarily have to be text-based, we included 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 [12]. We used these systems to introduce the concept of shoulder surfing attacks, and to discuss questions relating to password memorability. Our goal in this activity was to encourage students to think critically about how risks change in different system, and to use novel password systems to help students question their assumptions surrounding text passwords.

In the first part of this activity, students created a pattern lock password on an Android smartphone, and tried to see how easy it was to shoulder-surf their partners' pattern. We also asked them to see if they could guess the password from the smudge pattern left on the screen after their partner had unlocked the phone. In the second part of the activity, students tested out three variations of PassTiles, and explored the memorability of each. Since PassTiles is designed to make system-assigned passwords memorable, we asked students to consider why it might be more secure to assign passwords, and to relate this to usability problems.

3.2.4 Personal Knowledge Questions

In addition to regular authentication, we also wanted to discuss fallback authentication. A common method of fallback authentication is *personal knowledge questions* which ask the user to fill in answers to personal questions. These questions are meant to be designed to be easy for a user to answer about themselves, but difficult for another person to guess. However, the information requested is often easily obtained, and thus easily attacked.

In this activity, we created fake personal knowledge questions (and answers) for five celebrities. We asked students to see how many of the questions they could answer by googling for information. We chose questions that highlighted different problems with these types of questions, including questions with limited answer sets ("What is your favourite colour?"), questions with answers that are easily searched ("What city were you born in?"), and questions with unmemorable answers ("What is your favourite book?"). We also included one question that was very difficult to search ("What was your first phone number?") We fabricated answers to these questions.

In the accompanying worksheet, we asked students to relate their findings in the activity to including personal information in passwords, and why that is not recommended. We also asked students to consider these questions in relation to their own passwords and accounts, and to consider what avenues could be used to determine personal information about them.

3.2.5 Biometrics

Biometric authentication is seeing wide deployment in the form of fingerprint readers on smartphones, and because of this we felt it was important to include an activity about biometrics. In this activity, students created a silicone copy of their own fingerprint, and attempted to use it to unlock their smartphone (or a demo smartphone, if they did not have a smartphone with a fingerprint reader). Using commercially available modeling silicone (we used Smooth-On Body Double silicone[3]), we had students create a detailed model of the fingerprint. Students then dusted the silicone model with graphite powder to make it conductive, and could then use it to unlock their smartphone. To minimize complexity, we chose to have students make a cast directly from their finger, whereas in a real attack, an attacker would have to lift the fingerprint from another surface before making the cast. To demonstrate to students that this can be done, we had them place their fingerprints on transparencies, then invert a plastic cup dotted with superglue over the fingerprint. As the glue dissipates and dries, it reveals the fingerprint.

Owing to inconsistencies in how the component materials were mixed, and the care with which students created their casts, only some of the fingerprint models would actually unlock a phone, but the models were all detailed enough to convey to students that accurate copies of fingerprints can be relatively simply constructed. In this activity, we used the fingerprint models to direct students' attentions to the privacy issues incumbent in biometrics, and that although a fingerprint can identify you, it is not necessarily a secret. We also used the models to help students reason about issues such as credential revocation, and usability. At the end of the activity, we directed students to destroy the models.

3.3 Pilot Testing in Schools

Between October 2016 and January 2017, we pilot tested our authentication unit and activities in three Zürich-area gymnasiums. At the invitation of classroom teachers, we conducted workshops with four groups of students. As the purpose of this paper is to discuss our experiences designing and teaching the program, we will not discuss in detail any results of the workshops, but we think it is helpful to overview the environments in which we tested the prototype curriculum.

Group A was a class of 17 students enrolled in a gymnasium program specializing in languages. They were

[3] https://www.smooth-on.com/product-line/body-double/

in the 9^{th} class (aged approximately 14–15 years old). We were given a full day to spend with them, and we tested the entire activity set listed above. At the teacher's suggestion, we also had each group of students create a poster about one of the activities, and present those posters to the class during the discussion at the close of the workshop. Because these students were native German speakers, we translated the materials and the workshop was led by a native Swiss German speaker.

Group B was a class of 25 students enrolled in a gymnasium program specializing in applied mathematics, and were also in the 9^{th} class. We had a half-day timeslot in this classroom, and we conducted a shorter version of the workshop, keeping the round robin structure but using only the activites on creating good passwords, cracking passwords, and biometrics. We also conducted this workshop in German.

Group C was a class of 12 students enrolled in a gymnasium program specializing in mathematics and natural sciences. They were in the 11^{th} class (aged approximately 17 years). We were invited to spend 90 minutes with these students, and we conducted only the biometrics activity with this group. Given the older students in this group, we integrated some additional discussion and exploration of the issues inherent in biometric authentication. This workshop was conducted in English, though we distributed the materials in German.

The fourth workshop was conducted as part of a special activity week at the mathematics and natural sciences gymnasium. Students from different grade levels could choose different workshops in which to participate during the week. Group D was a group of about 30 students ranging in age from 16 to 18 years old and coming from different classrooms. We were given another 90 minute slot, and we again conducted the introduction to authentication together with the biometrics activity. We conducted this workshop in a mixture of English and German, with German materials distributed.

The pilot tests helped us refine our activities and better understand the abilities of the high school audience we were targeting. Following the pilot tests, we modified some of the mathematical content (*e.g.* removing references to factorials when we found that students had not yet learned about them), adjusted the length of worksheets, and edited instructions for clarity. We added content to address timing problems (*e.g.* adding the fingerprint reveal activity to occupy students while the silicone molds were drying).

Apart from the biometrics activity, students were mostly able to follow the directions given and to understand the activities without leadership from teachers. Predictably, the messy nature of the biometrics activity distracted students from both the instructions and the followup questions. As activity leaders, we also gave a certain amount of advice around how to mix and apply the materials and about when the materials were sufficiently dry to proceed, and this kind of feedback resulted in the biometrics activity being less student-led than the other activities.

Even though our groups of students were relatively uniform, we saw dramatic differences between groups in mathematical knowledge, language ability, computer science background, and classroom dynamics. While such differences are to be expected, they emphasized for us the importance of creating material that is easily adapted to different situations, classrooms, and backgrounds.

4 Challenges of Security Education

Based on our experiences designing these curriculum materials and pilot testing them in schools, we identified a number of challenges affecting the design and evaluation of security education programs. We contend that many of these challenges stem directly from the properties of security, and are inherent to teaching security. Rather than being problems that affect only our prototype curriculum, these problems are general problems that arise in designing security education.

4.1 The Bleeding Edge

Security technologies are continually changing. Even over the course of our project, changes to authentication systems took place, affecting what we decided to present and teach. This means that we need to develop extensible lessons about security, that include the idea that users might be called to extend the concepts learned in one context to a new technology.

Our biometrics activity was particularly affected by these changes. Because of the recent and widespread deployment of fingerprint readers and face recognition on mobile devices, we felt it was extremely important to discuss the implications of using these technologies, but were hampered by the fact that deployment is ongoing and the future is unclear.

The constant changes in security technology are a result of burgeoning technological development, but also stem from the presence of the adversary in computer systems. Because of attackers, security is unlikely ever to be a static topic. In teaching security, we need to emphasize the idea that the landscape will shift, but that the principles will remain. Related to this is the idea that because of the attacker, different security technologies should be evaluated differently in different scenarios. In one of our workshops, a student mentioned that his house had a door lock that used fingerprints to unlock. He was able to identify different advantages and disadvantages in using biometrics for this purpose, including usability problems that rarely arose on the phone (*e.g.* using it in the rain), and the idea of a different form of recovery authentication (housekey vs. PIN). This emerging technology was an excellent example of how fingerprint authentication should be considered differently in different scenarios, but without student-led examples, it can be difficult to emphasize these points.

4.2 When to Teach Security?

A question that arose as we planned our modules was when to introduce different topics. Is there a right moment to discuss security topics? Children typically progress quickly from having mediated online access [18] to having multiple accounts and a great deal of online independence. The knowledge we are imparting should be useful to students at any stage, but identifying a moment where the material is relevant and students are developmentally ready can be tricky. One tension we identified was that students might not be interested in passwords and security when they have nothing to protect online, but that it is effectively too late to teach these lessons when students have already formed misconceptions or bad habits around security.

This is another instance where the shifting landscape of technology use deeply affects how we teach about security. Children are getting increased access to devices and accounts earlier in life [9], but it is hard to know at what point children start to feel personal responsibility for, and investment in their own online presence. There are also environmental factors that affect this weighting – different socioeconomic groups or cultural factors might influence the extent and age at which children are given online access.

4.3 Practical vs. Theoretical

Security is a technical subject; much of it rests on relatively advanced mathematical concepts. Often too, "the devil is in the details", and small differences in setup can deeply affect the security of a system. The line between practical and theoretical security can be difficult to discern, and determining how much theoretical knowledge is needed to underpin the practical takeaway can be difficult.

The practical takeaways of security often seem almost tangential to computer science curriculum. An analogy might perhaps be the relationship between Newton's laws of motion and why people should be careful crossing the street. Someone does not need to know that $F = m \times a$ in order to understand that a truck could flatten them. And yet at the same time, it appears that not knowing any of the background leads users to overinterpret the metaphors of security and create problematic mental models that fail to help them reason about the future [16].

In our work, we decided to limit our involvement in the details of security. We took the liberty of ignoring details when we thought they would complicate the story. We were prepared to discuss them if asked, but in general, we focused our activities on the concepts of attacks, rather than the implementation details. Particularly in the password cracking activity, we elided several related issues that would have complicated the scenario and setup. We did not explicitly explain offline attacks, and did not discuss the concept of safe password storage on the back end. We avoided explaining the concepts of encryption or hashing, opting instead to describe the hashed passwords as "disguised". Though encryption and offline attack strategies are interesting topics, we chose to keep our focus on the parts of the material that could directly impact how end users choose their passwords and protect their accounts.

4.4 Giving Clear Advice

As much as our goal was to deliver practical advice about passwords, when developing materials we struggled in settling on straightforward advice about security. Security is notoriously difficult to distill into pithy rules of thumb [8]. It is hard to make sweeping statements and guarantees about security, and often difficult to explain the subtle interplay of factors (relating to both security and usability) that goes into good decision-making about security.

One criticism of much security advice is that it is quick to tell users what they should *not* do, but is less helpful on the topic of what they should do. Security advice may also be too general to be much help - telling users to create long passwords is unhelpful if "long" is not defined. But, understanding the adversarial nature of security, security experts understand that putting a firm requirement on password length is impossible, and dependent on many features that cannot be evaluated. This was part of why we tried to emphasize the notion of attacks and defences in our materials. Understanding that an attack may be possible, and having some notion of attackers' typical strategies and capabilities gives users tools to make realistic choices about security. Framing passwords as defences against attacks also implies the idea that some accounts need to be better defended than others, and that special attention should be paid to them.

Another problem in giving security advice is that some advice does not apply equally to all accounts. In an ideal world, users would create long, random, and unique passwords for all accounts. In reality, users have many accounts, and following this advice would effectively overload users' time and capacity for handling passwords. In our activities, we deliberately avoided the topic of password reuse attacks, on the basis that we did not think it was particularly helpful to emphasize this risk to users. Without going as far as saying it, users probably *should* reuse passwords – and it is better to reuse a strong password than to create myriad weak passwords. Avoiding this topic was possibly a lazy way out of the problem, but we found that it was difficult to impart the nuance required to debate these kinds of issues in the context of the classroom.

The biometrics activity was another activity where we found it difficult to give straightforward answers to questions about how and whether these technologies should be used. We wanted students to be aware of the privacy and revocation concerns inherent to biometric technologies, and there are certainly issues that will arise when biometrics are used in many situations, but we did not want to tell users to stop using the fingerprint sensors on smartphones, where the risks are manageable and the usability advantages are undeniable.

4.5 Too Easy ... or Too Hard

One problem that we encountered in putting together these modules was how to balance the complicated details with the practical rules that they imply, which often appear trivially simple. We had difficulty finding a balance between these poles of "too easy" and "too hard". In both cases, students exhibited boredom with the material, but finding an engaging intersection of the spheres proved to be difficult. We decreased the mathematical content of the activity about creating good passwords when we found that students were having difficulty relating the password space calculations to the concepts of guessing time. Our intention had been that reasoning about the equation would allow students to consider the password features that would most effectively protect against attacks, but we found that students did not have the skills to use the mathematical equation as a tool for reasoning about passwords.

4.6 Who should teach security?

Although we developed our materials with the idea that they should be self-sufficient and accessible for teachers to develop, we accompanied them and took on the role of teachers in our pilot workshops. We found that though students were mainly able to follow and complete the activities themselves, we were still needed to conduct discussions and challenge students to consider the issues at hand. Particularly in the discussions that we conducted around the biometrics activity, we talked about tradeoffs between privacy, security, and usability, and encouraged students to consider when these tradeoffs might and might not be appropriate.

The issue of who should teach security is thorny. Teachers are not, and will continue not to be, experts in security. There is no reason that they could not teach security, but adding this complex body of knowledge to the lengthy list of subjects they must master seems burdensome. Without training, there is also the concern that teachers will perpetrate the kinds of security misconceptions that are seen in studies of adult users. We suggest that security education materials need to be either completely independent, or should come with specific training materials for teachers.

4.7 Measuring Success

Our high level goal in designing this curriculum was to help educate users to be more secure over their lifetimes. Operationalizing this goal to measure the success of our workshops proved to be difficult. Ideally, we would like to see decreases in security breaches over a large-scale, longitudinal data set, but obtaining this data is difficult. This problem is compounded by the separation between action and consequence in security decision-making. It is difficult to know how individual actions impact security outcomes, both at the macro and micro levels, and collecting data about account breaches and the corresponding personal losses is out of reach in a classroom setting.

In the pilot tests described here, we were seeking feedback on the units themselves, and trying to understand where they were successful and where unsuccessful. We were concerned with evaluating the clarity of the instructions, fine-tuning the length of the activities, calibrating the appropriateness of the material, and iterating to improve the design of the workshop. For this reason, we chose not to evaluate students' performance in any way. But upon reflection, we increasingly believe that measuring students' performance in this area is essentially meaningless. What can be evaluated in the context of the classroom that will give a valid indication of the success of the program? For some activites, a pre-test/post-test design could be used to test improvements in created passwords, but other issues, such those relating to the privacy of biometrics, are more difficult to measure in this model.

5 Discussion

Taken together, the challenges that we outline here indicate that the approach to teaching security in high schools needs to be carefully considered. Security curriculum is important and necessary, but may not integrate well with other subjects taught in secondary schools. The constraints of the secondary school audience also affect the priorities in teaching security, and place an emphasis on practical risk management.

Much of the challenge of teaching practical security skills is in teaching risk assessment. Although there is applicable technical information and knowledge of threats and defences that can help, much of teaching about security involves asking students to make judgements about where and when different security behaviours are applicable. It is our hope that presenting age-appropriate material about computer security, motivated by relatable scenarios, will help students to make these judgments. We also think that this emphasis on risk assessment means that computer security topics need to be revisited over the entire secondary school curriculum, perhaps once or twice per year.

Another finding from our experience in developing and testing the authentication module is that the needs of teaching to secondary school students are different from those of the university undergraduates often featured in the academic literature. Secondary school students are not necessarily interested in computer science, and may have little to no technical background about the Internet. They are also at an age where they are gaining independence and control over personal data and social relationships, making this a crucial time to emphasize the importance of good security practices.

Based on the challenges, constraints, and importance of teaching security, we think that an effective approach to teaching it may be to follow the practices of sex education or other safety education programs. There are a number of parallels between security education and sex/health education and we conjecture that examining the ways in which programs have been implemented might offer a useful avenue for designing security education programs.

Security and sexual health are both areas in which people are asked to make risk assessments. Both areas offer risk and reward. Particularly for teenagers, both are attractive activities, in spite of the associated risks. While the risks of unprotected sexual activity are in some respects more concrete than those of using the Internet, both are probabilistic risks. We are unlikely to fully discourage teenagers from either activity, but it is crucial that they are made aware of the risks and given tools to reason about dangers and how to protect against them.

From the perspective of curriculum development, security and sex/health education also have parallels. They are both subjects that relate to academic topics (informatics and biology), but are not the primary application of those subjects. They should both be revisited periodically, but are not part of the main focus of the curriculum. They are both subjects which teachers may feel uncomfortable or unsuited to teaching. Neither subject lends itself well to classroom evaluation.

Moving forward, we believe that a deeper exploration of parallels and lessons learned from this existing domain could benefit the development of security education programs for secondary schools.

6 Conclusion

In this paper we outlined our experiences in developing curriculum material on user authentication for use in Swiss secondary schools. We created five interactive, student-led activities to teach about various aspects of authentication. Our goal was to address gaps in security knowledge that are seen in adult audiences. Our approach was to teach about the threats and defences affecting passwords, in the hope that this would encourage students to view security as an ongoing exercise in risk management. From our experience pilot testing these materials in schools, we encountered and identified a number of challenges that we believe are inherent to teaching security. Based on these challenges, we suggest that a productive approach to teaching computer security might be to follow the lead of high school sex education programs, which address many similar challenges.

The program described here is work in progress, and is far from representing a mature curriculum for computer security in high schools. However, it is sufficient to highlight the challenges that are inherent to teaching computer security in secondary schools. We do not mean to suggest that these challenges are necessarily unique to secondary schools, and they may well apply to primary school and even adult-oriented security education programs, but that there are differences in how security education needs to be approached between university programs and more general education programs. In future work, we hope that we (and others) will be able to develop more extensive activities and materials that approach computer security from the perspective of public health and safety.

7 Acknowledgments

We would like to extend our thanks to Ivana Kosirova, Michael Bürgisser, Jens Maue, and Lukas Fässler for inviting us into their classrooms and supporting our work. We would also like to thank Tobias Kohn and Urs Hauser for their valuable feedback on our teaching materials, Stephanos Matsumoto for his assistance, and Srdjan Capkun and Juraj Hromkovic for their support of the project. And of course we could not have pursued this work without the generous and enthusiastic participation of the students in our workshops.

References

[1] Assal, H., Imran, A., and Chiasson, S. An Exploration of Graphical Password Authentication for Children.

[2] boyd, d. *It's Complicated: The Social Life of Networked Teens*. Yale University Press, 2014.

[3] Coggins, P. E. Implications of What Children Know About Computer Passwords. *Computers in the Schools 30* (2013), 282–293.

[4] Florencio, D., and Herley, C. A Large-Scale Study of Web Password Habits. In *International World Wide Web Conference Committee* (Banff, Canada, 2007).

[5] Florencio, D., Herley, C., and van Oorschot, P. C. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In *Proceedings of the 23rd USENIX Security Symposium* (San Diego, USA, Aug. 2014).

[6] Herley, C. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms* (2009), ACM.

[7] Herley, C., and van Oorschot, P. C. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy Magazine 10*, 1 (2012), 28–36.

[8] Ion, I., Reeder, R. W., and Consolvo, S. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *SOUPS '15* (July 2015), pp. 1–20.

[9] May-Chahal, C., Mason, C., Rashid, A., Walkerdine, J., Rayson, P., and Greenwood, P. Safeguarding Cyborg Childhoods: Incorporating the On/Offline Behaviour of Children into Everyday Social Work Practices. *British Journal of Social Work 44*, 3 (Apr. 2014), 596–614.

[10] Read, J. C., and Cassidy, B. Designing textual password systems for children. In *the 11th International Conference* (2012), ACM, pp. 200–203.

[11] Steves, M., Chisnell, D., Sasse, M. A., Krol, K., Theofanos, M., and Wald, H. Report: Authentication Diary Study. Tech. rep., National Institute of Standards and Technology, Information Technology Laboratory, Gaithersburg, MD, Feb. 2014.

[12] Stobert, E., and Biddle, R. Memory retrieval and graphical passwords. In *Proceedings of the 9th Symposium on Usable Privacy and Security* (Newcastle, UK, 2013), ACM.

[13] Stobert, E., and Biddle, R. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS)* (2014), USENIX.

[14] Ur, B., Habib, H., Johnson, N., Melicher, W., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L. F., Dixon, H., and Emami Naeini, P. Design and Evaluation of a Data-Driven Password Meter. In *the 2017 CHI Conference* (New York, New York, USA, 2017), ACM Press, pp. 3775–3786.

[15] Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., and Cranor, L. F. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proceedings of the 21st USENIX Security Symposium* (Aug. 2012), USENIX Association.

[16] Wash, R. Folk Models of Home Computer Security. In *Proceedings of the 6th Symposium on Usable Privacy and Security* (July 2010), ACM.

[17] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., and Memon, N. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *International Journal of Human-Computer Studies 63*, 1-2 (July 2005), 102–127.

[18] Zhang-Kennedy, L., Mekhail, C., Abdelaziz, Y., and Chiasson, S. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *IWC 2016* (Mar. 2016), pp. 1–12.