Proposed New Course:
Usable Security and Privacy (USec)

Kami Vaniea

March 25, 2018

PROPOSED COURSE TITLE: Usable Security and Privacy
PROPOSER(S): Kami Vaniea
DATE:

1 SECTION 1 - CASE FOR SUPPORT

[This section should summarize why the new course is needed, how it fits with the existing course portfolio, the curricula of our Degree Programmes, and delivery of teaching for the different years it would affect.]

1.1 Overall contribution to teaching portfolio

[Explain what motivates the course proposal, e.g. an emergent or maturing research area, a previous course having become outdated or inappropriate in other ways, novel research activity or newly acquired expertise in the School, offerings of our competitors.]

The area of Usable Security and Privacy is a growing area that is seeing growing recognition for its role in creating secure systems. Edinurgh has an opportunity to to set ourselves appart in our offerings by providing a course that targets this area.

More generally, the course would grow our offering in the Security/Privacy area and assist in the creation of a Security and Privacy MSc with the possibly of a National Cyber Security Center (NCSC) accreditation. It would also extend the offerings in Human-Computer Interaction which is also a growing area in the school. It would also add a privacy course to our offering which is currently missing and possibly of great interest to Data Science students.

1.2 Target audience and expected demand

[Describe the type of student the course would appeal to in terms of background, level of ability, and interests, and the expected class size for the course based on anticipated demand. A good justification would include some evidence, e.g. by referring to projects in an area, class sizes in similar courses, employer demand for the skills taught in the course, etc.]

Expected class size is between 60 and 100, though it could go higher. The number of students who meet the pre-requisites is quite large since Computer Security is now required in UG3 for several DPs and the Human-Computer course regularly has over 100 students. The Human Factor course has 160 students this year, suggesting that a S2 course that builds on HCI has the potential to attract students. Similarly the Computer Security course had 160 students this year, before it was made required, again speaking to the popularity of the topic.

The course targets students with a background in computer security or human computer interaction. It would provide a lighter introduction to two important topics for students who either are not interested in the hacking skills associated with Computer Security or consider Human-Computer Interaction to be too design focused.

1.3 Relation to existing curriculum

[This section should describe how the proposed course relates to existing courses, programmes, years of study, and specialisms. Every new course should make an important contribution to the delivery of our Degree Programmes, which are described at http://www.drps.ed.ac.uk/17-18/dpt/drps_inf.htm. Please name the Programmes the course will contribute to, and justify its contribution in relation to courses already available within those programmes. For courses available to MSc students, describe which specialism(s) the course should be listed under (see http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2017/programme-guide/specialist-areas), and what its significance for the specialism would be. Comment on the fit of the proposed course with the structure of academic years for which it should be offered. This is described in the Year Guides linked from http://web.inf.ed.ac.uk/infweb/student-services/ito/students.]

The course relates to several different degree programs:

Both Cyber Security and Human Computer Interaction are cross-disciplinary topics which relate to nearly every area of computer science.

Cyber Security is putting together an MSc and a CDT, both of which view UPS as an important part of their course offerings.

Data Science as well as several other CDTs are getting pressure to include more topics around security, ethics, and privacy. This course would provide some of that discussion.

1.4 Resources

[While course approvals do not anticipate the School's decision that a course will actually be taught in any given year, it is important to describe what resources would be required if it were run. Please describe how much lecturing, tutoring, exam preparation and marking effort will be required in steady state, and any additional resources that will be required to set the course up for the first time. Please make sure that you provide estimates relative to class size if there are natural limits to its scalability (e.g. due to equipment or space requirements). Describe the profile of the course team, including lecturer, tutors, markers, and their required background. Where possible, identify a set of specific lecturers who have confirmed that they would either like to teach this course apart from the proposer, or who could teach the course in principle. It is useful to include ideas and suggestions for potential teaching duty re-allocation (e.g. through course sharing, discontinuation of an existing course, voluntary teaching over and above normal teaching duties) to be taken into account when resourcing decisions are made.]

Course Lecturers: The course would primarily be taught by Kami Vaniea. We anticipate that the first year would be video recorded, after which it would be possible for other Lecturers with some experience in the area to teach it as well, such as David Aspinal.

Background Videos: The initial set of videos will be pulled from existing lecture recordings in both Human Computer Interaction and Computer Security. As these videos already exist and only need to be trimmed, I anticipate that the time cost will not be large. The created videos should also be fairly stable between years.

Tutorials: Assuming the course has more than 50 students enrolled (likely) we will have tutorial sessions where students can engage with and discuss course material. Similar to HCI, the tutorials will be on the large side with 10-15 students. This is an intentional decision so they can form groups and do in-tutorial activities that help them engage with the material while being guided by a tutor.

TAs and Markers: Markers will need an HCI background. The lecturer, or a PhD student with Usable Security and Privacy knowledge will also have to be involved in the marking to help with odd marking cases, especially on the security side.

2 SECTION 2 - COURSE DESCRIPTOR

[This is the official course descriptor that will be published by the University and serves as the authoritative source of information about the course for student via DRPS and PATH. Current course descriptions in the EUCLID Course Catalogue are available at www.euclid.ed.ac.uk under "DPTs and Courses", searching for courses beginning 'INFR']

2.1 Course Title:

Usable Security and Privacy

2.2 SCQF Credit Points:

[The Scottish Credit and Qualifications Framework specifies where each training component provided by educational institutions fits into the national education system. Credit points per course are normally 10 or 20, and a student normally enrols for 60 credits per semester. For those familiar with the ECTS system, one ECTS credit is equivalent to 2 SCQF credits. See also http://www.scqf.org.uk/The

10

SCQF Credit Level: [These levels correspond to different levels of skills and outcomes, see http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdf At University level, Year 1/2 courses are normally level 8, Year 3 can be level 9 or 10, Year 4 10 or 11, and Year 5/MSc have to be level 11. MSc programmes may permit a small number (up to 30 credits overall) of level 9 or 10 courses.]

11

Normal Year Taken: 1/2/3/4/5/MSc
While a course may be available for more than one year, this should specify when it is normally taken by a student. "5" here indicates the fifth year of undergraduate Masters programmes such as MInf.

4

Also available in years: 1/2/3/4/5/MSc
Different options are possible depending on the choice of SCQF Credit Level above: for level 9, you should specify if the course is for 3rd year undergraduates only, or also open to MSc students (default); for level 10, you should specify if the course is available to 3rd year and 4th year undergraduates (default), 4th year undergraduates only, and whether it should be open to MSc students; for level 11, a course can be available to 4th and 5th year undergraduates and MSc students (default), to 5th year undergraduates and MSc students, or to MSc students only]

5, MSc

Undergraduate or Postgraduate? [If the course is only available to MSc students, then it must be classified as a Postgraduate course. All other courses, regardless of level, will be classified as Undergraduate]

Undergraduate

2.3 Subject Area and Specialism Classification:

[Any combination of Computer Science, Artificial Intelligence, Software Engineering and/or Cognitive Science as appropriate. For courses available to MSc students, please also specify the relevant MSc specialist area (to be found in the online MSc Year Guide at http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2017/programme-guide/specialist-areas), distinguishing between whether the course should be considered as 'core' or 'optional' for the respective specialist area.]

Computer Science, Artificial Intellilgence, Software Engineering, Cognitive Science
MSc Specialisms:

- Cyber Security and Privacy (core)

- Data Science (optional)
- Cognitive Science (optional)
- Computer Systems, Software Engineering and High-Performance Computing (optional)
- Agents, Knowledge and Data (optional)
- Informatics

Appropriate/Important for the Following Degree Programmes: [Please check against programmes from http://www.drps.ed.ac.uk/17-18/dpt/drps_inf.htm to determine any specific programmes for which the course would be relevant (in many cases, information about the Subject Area classification above will be sufficient and specific programmes do not have to be specified). Some courses may be specifically designed for non-Informatics students or with students with a specific profile as a potential audience, please describe this here if appropriate.]

The course is not aimed at a specific Degree Program

Timetabling Information: [Provide details on the semester the course should be offered in, specifying any timetabling constraints to be considered (e.g. overlap of popular combinations, other specialism courses, external courses etc).]

Second semester.

It would be best if it happened the semester after HCI so that the most number of students could have a chance to take the prerequisites. Also, because it is a more advanced HCI course so there is a natural progression from HCI to this course.

2.4 Summary Course Description:

[Provide a brief official description of the course, around 100 words. This should be worded in a student-friendly way, it is the part of the descriptor a student is most likely to read.]

Humans are a vital component of secure and private systems, they are also one of the most expensive components and the most challenging to reason about. In this course, students will learn about how to create systems that are usable while still fulfilling their primary security or privacy mission. Students will also learn about research topics such as designing user studies to critically evaluate interfaces and reading academic papers to create an academically-informed view of the topic.

Course Description: [Provide an academic description, an outline of the content covered by the course and a description of the learning experience students can expect to get. See guidance notes at: http://www.studentsystems.is.ed.ac.uk/staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

- Introduction: History and overview of the Usable Security and Privacy research area including the transition from blaming users to treating them as valued components of a secure system.
- Study design: Security and privacy activities tend to be secondary tasks. The student will learn how to design and analyze usability studies that are common in security and privacy such as targeting secondary tasks or using some deception.
- Privacy: Basic overview of the definitions of privacy as well as some of the legal and social aspects of it. Analysis of common privacy issues and how they are expressed through user interaction with systems.
- Security: Overview of common security technologies and how they are impacted by usability. In-depth look at select topics such as password construction and management.
- Ethics: Discussion of ethics, particularly around research in topics in security and privacy where participants can be particularly vulnerable.

Pre-Requisite Courses: [Specify any courses that a student must have taken to be permitted to take this course. Pre-requisites listed in this section can only be waived by special permission from the School's Curriculum Approval Officer, so they should be treated as "must-have". By default, you may assume that any student who will register for the course has taken those courses compulsory for the degree for which the course is listed in previous years. Please include the FULL course name and course code].

Students must have taken a Human-Computer Interaction course OR a Computer Security course previously. Courses from other universities are acceptable; however, students are advised to consult the course website to make certain that their prior courses have covered the necessary material.

Co-Requisite Courses: [Specify any courses that should be taken in parallel with the existing course. Note that this leads to a timetabling constraint that should be mentioned elsewhere in the proposal. Please include the FULL course name and course code].

none

Prohibited Combinations: [Specify any courses that should not be taken in combination with the proposed course. Please include the FULL course name and course code].

none

Other Requirements: [Please list any further background students should have, including, for example, mathematical skills, programming ability, experimentation/lab experience, etc. It is important to consider that unless there are formal prerequisites for participation in a course, other Schools can register their students onto our courses, so it is important to be clear in this section. Also be aware that MSc students are unlikely to have the pre-requisite courses, so alternative knowledge should be recommended. If you want to only permit this by special permission, a statement like "Successful completion of Year X of an Informatics Single or Combined Honours Degree, or equivalent by permission of the School." can be included.]

A general familiarity with computer science and programming are recommended.

Available to Visiting Students: Yes

[Provide a justification if the answer is No.]

2.5 Summary of Intended Learning Outcomes (MAXIMUM OF 5):

Commented [MV1]: Amended by DoT/SoA for approval by Convenors action 03/04/18

[List the learning outcomes of the course, emphasizing what the impact of the course will be on an individual who successfully completes it, rather than the activity that will lead to this outcome. Further guidance is available from https://canvas.instructure.com/courses/801386/files/24062695]

1. Basic understanding of key topics in Security, Privacy, and Human-Computer Interaction.
2. Be able to identify "privacy" and "security" concerns in different contexts.
3. Critically evaluate the literature to develop an academically-informed view of proposed security and privacy solutions from a human factors perspective.
4. Design studies to rigorously evaluate the usability of a security or privacy tool.
5. Apply techniques and design approaches to security and privacy problems to create usable solutions.

Assessment Information [Provide a description of all types of assessment that will be used in the course (e.g. written exam, oral presentation, essay, programming practical, etc) and how each of them will assess the intended learning outcomes listed above. Where coursework involves group work, it is important to remember that every student has to be assessed individually for their contribution to any jointly produced piece of work. Please include any minimum requirements for assessment components e.g. student must pass all individual pieces of assessment as well as course overall].

Assessment Weightings:

Written Examination: 80%
Practical Examination: 0%
Coursework: 20%

Time spend on assignments: [Weightings up to a 70/30 split between exam and coursework are considered standard, any higher coursework percentage requires a specific justification. The general expectation is that a 10-point course will have an 80/20 split and include the equivalent of one 20-hour coursework assignment (although this can be split into several smaller pieces of coursework. The Practical Examination category should be used for courses with programming exams. You should not expect that during term time a student will have more than 2-4 hours to spend on a single assignment for a course per week. Please note that it is possible, and in many cases desirable, to include formative assignments which are not formally assessed but submitted for feedback, often in combination with peer assessment.]

20 hours on assessed coursework.

Academic description: [A more technical summary of the course aims and contents. May include terminology and technical content that might be more relevant to colleagues and administrators than to students.]

Syllabus: [Provide a more detailed description of the contents of the course, e.g. a list of bullet points roughly corresponding to the topics covered in each individual lecture/tutorial/coursework. The description should not exceed 500 words but should be detailed enough to allow a student to have a good idea of what material will be covered in the course. Please keep in mind that this needs to be flexible enough to allow for minor changes from year to year without requiring new course approval each time.]

- History of security and usability (Introduction)
- Privacy
- Warning design
- Phishing
- Study design
- Research ethics
- Authentication mechanisms
- Public/Private key management and email security
- Device pairing
- Data usage and privacy policies
- Mobile Security and privacy including location and permissions
- Usability for developers and system administrators

Relevant QAA Computing Curriculum Sections: [Please see http://www.qaa.ac.uk/en/Publications/Documents Computing-consultation-15.pdf to check which section the course fits into.]

Human-computer interaction, Software engineering

Note: Software engineering was selected because it is the only QAA section to mention security.

Graduate Attributes, Personal and Professional skills: [This field should be used to describe the contribution made to the development of a student's personal and professional attributes and skills as a result of studying this course i.e. the generic and transferable skills beyond the subject of study itself. Reference in particular should be made to SCQF learning characteristics at the correct level http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdf].

- Be able to identify and handle situations involving potential breaches of privacy and ethics.
- Develop skills reading research papers and critically analyzing their study methodologies.

- Be able to transfer knowledge from an academic paper to a real world scenario.
- Apply critical analysis, evaluation and synthesis to issues that are in- formed by forefront developments in the subject/discipline/sector

Reading List: [Provide a list of relevant readings. See also remarks under 3d.]
Required readings will be primarily from open access papers listed on the course website. The below readings [1] and [2] are textbooks which summarize key research papers in the area and are therefore highly recommended. [3] and [4] are the textbooks for Computer Security and HCI respectfully and are recommended for students who need more background in those subjects.

1. Usable Security: History, Themes, and Challenges by Simson Garfinkel and Heather Richter Lipford
2. Security and Usability: Designing Secure Systems that People Can Use by Lorrie Cranor and Simson Garfinkel
3. Introduction to Computer Security Goodrich et al.
4. Human-Computer Interaction by Dix, Finlay, Abowd and Reale

Breakdown of Learning and Teaching Activities: [Total number of lecture hours and tutorial hours, with hours for coursework assignments.] [The breakdown of learning and teaching activities should only include contact hours with the students; everything else should be accounted for in the Directed Learning and Independent Learning hours. The total being 10 x course credits. Assume 10 weeks of lectures slots and 10 weeks of tutorials, though not all of these need to be filled with actual contact hours. As a guideline, if a 10-pt course has 20 lecture slots in principle, around 15 of these should be filled with examinable material; the rest should be used for guest lectures, revision sessions, introductions to assignments, etc. Additional categories of learning and teaching activities are available, a full list can be found at: http://www.euclid.ed.ac.uk/Staff/Support/User_Guides/CCAM/Teaching_Learning.htm]

Lecture Hours: 18 hours

Seminar/Tutorial Hours: 3 hours

Summative assessment hours: 20 hours

Feedback/Feedforward hours: 2 hours

Programme Level learning and Teaching hours: 2 hours

Directed Learning and Independent Learning hours: 50 hours

Total hours: 95 hours

You may also find the guidance on Total Contact Teaching Hours and Examination & Assessment Information at: http://www.studentsystems.ed.ac.uk/Staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

Keywords: [A list of searchable keywords.]
Human-Computer Interaction, Cyber Security, Privacy, Human Factors of Privacy and Security, Usable Security and Privacy

3 SECTION 3 - COURSE MATERIALS

3.1 Sample exam question(s)

[Sample exam questions with model answers to the individual questions are required for new courses. A justification of the exam format should be provided where the suggested format non-standard. The online list of past exam papers gives an idea of what exam formats are most commonly used and which alternative formats have been http://www.inf.ed.ac.uk/teaching/exam_papers/.]

See Appendix A for the example exam question.

The exam would be the standard choose two of three format used by Informatics. The structure would likely focus on the three main conceptual areas of this type of research: 1) analysis of an existing security or privacy interface to identify why it is or is not usable, 2) design of a new interface that fits both the technical security requirements and usability best practices, 3) design of an evaluation that will formally test the usability in the context of common security issues such as security as a secondary task, or complex concepts like key servers.

Similar to HCI, I will be formally asking the ITO to allow pencils for the drawing of interfaces on exams. But otherwise the exam will follow standard Informatics structure.

3.2 Sample coursework specification

[Provide a description of a possible assignment with an estimate of effort against each sub-task and a description of marking criteria.]

The coursework will involve the student selecting a security or privacy technology from a provided short list, conducting a self assessment of it, and then designing a study that will test the usability of that technology. The result will be a writeup, including all the material from the study design.

The coursework will involve standard readily available security and privacy technologies such as Enigmail (email encryption plugin), browser password managers, UMatrix (Javascript manager), and Off the Record Messaging (instant messaging encryption plugin). Students will be provided with an option both so they can learn more about a technology they find interesting, and so that the markers get some variety. The technologies selected will all be smaller in nature and user facing which means that planned evaluations should all have a similar structure.

To keep the coursework reasonable for a 10 credit course, students will write up their own opinion of the usability and then design a that would verify or refute their theories, but not run the study. This structure is partially setup to compliment the HCI class where students put less effort into study design and more effort into running the study. A student taking both courses would therefore be evaluated on different skill sets.

For marking, the coursework will focus on the student's ability to assess the tool not only based on HCI principles, but also taking into account the security and privacy concepts the tool is built on. Anyone can make email encryption easy by simply removing all the key management elements, but doing so would destroy the security. Similarly, an HCI student my determinate that a tool as highly usable because it stores all private keys in the cloud while a usable security student is expected to realize that the interface is actually putting the user in danger. Students are expected to identify these types of issues on their own, and then design a study, including all the materials, that would test their theories about usability problems.

3.3 Sample tutorial/lab sheet questions

[Provide a list of tutorial questions and answers and/or samples of lab sheets.]

Tutorials will look similar to one below from HCI, though with different content. In tutorial students will be asked to conduct a mini study using a particular methodology in the presence of a tutor who can answer questions as they come up, and comment on the running of their study. At the end of the tutorial session the students then discuss the practiced methodology as a group.

http://www.inf.ed.ac.uk/teaching/courses/hci/1718/tuts/think_aloud.pdf

3.4 Any other relevant materials

[Include anything else that is relevant, possibly in the form of links. If you do not want to specify a set of concrete readings for the official course descriptor, please list examples here.]

4 SECTION 4 - COURSE MANAGEMENT

4.1 Course information and publicity

[Describe what information will be provided at the start of the academic year in which format, how and where the course will be advertised, what materials will be made available online and when they will be finalized. Please note that University and School policies require that all course information is available at the start of the academic year including all teaching materials and lecture slides.]

The course will be advertised in the Human Computer Interaction course which is first semester, it will also be advertised in the general MSc first semester security course when it gets approved.

4.2 Feedback

[Provide details on feedback arrangements for the course. This includes when and how course feedback is solicited from the class and responded to, what feedback will be provided on assessment (coursework and exams) within what time frame, and what opportunities students will be given to respond to feedback. The University is committed to a baseline of principles regarding feedback that we have to implement at every level, these are described at `http://www.docs.sasg.ed.ac.uk/AcademicServices/Policies/Feedback_Standards_Guiding_Principles.pdf`. Further guidance is available from http://www.enhancingfeedback.ed.a

Course feedback will be solicited mid-semester using paper forms. Feedback response will be given in lecture.

4.3 Management of teaching delivery

[Provide details on responsibilities of each course staff member, how the lecturer will recruit, train, and supervise other course staff, what forms of communication with the class will be used, how required equipment will be procured and maintained. Include information about what support will be required for this from other parties, e.g. colleagues or the Informatics Teaching Organisation.]

The TA will be responsible for helping prepare the coursework, particularly in the first year. Markers will need to be trained in HCI study design and will be drawn from HCI PhD students. Tutors will also be drawn from HCI trained students, possibly including Design Informatics MSc students. Tutorial content focuses more on HCI than on the usable security components so a student trained in that area would be able to tutor.

No special software or hardware is needed beyond what already exists on all DICE computers.

Communication with students will be done primarily through Piazza, with Learn used for some copyright concerning content and for the course videos.

5 SECTION 5 - COMMENTS

[This section summarises comments received from relevant individuals prior to proposing the course. If you have not discussed this proposal with others please note this].

5.1 Year Organiser Comments

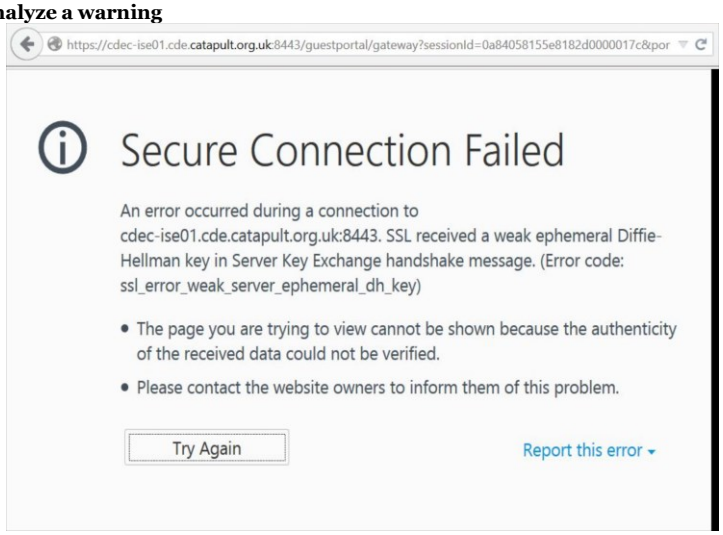
[Year Organisers are responsible for maintaining the official Year Guides for every year of study, which, among other things, provide guidance on available course choices and specialist areas. The Year Organisers of all years for which the course will be offered should be consulted on the appropriateness and relevance on the course. Issues to consider here include balance of course offerings across semesters, subject areas, and credit levels, timetabling implications, fit into the administrative structures used in delivering that year.]

5.2 BoS Academic Secretary

[Any proposal has to be checked by the Secretary of the Board of Studies prior to discussion at the actual Board meeting. This is a placeholder for their comments, mainly on the formal quality of the content provided above.]

A Example Exam Question

Analyze a warning



When trying to open a website the instructor received the above warning in her web browser.

SSL/TLS supports several cryptographic algorithms and during the initial handshake the browser and the server negotiate which one they will use. Some of these algorithms are older and no longer considered to be secure by the cryptographic community. The warning above is telling the user that the remote server is only willing to use an older insecure protocol, so the browser has blocked the connection for the user's safety.

1. Use the framework for reasoning about the human-in-the-loop discussed in class and pictured in Figure 1 to analyze the usability of the warning.
2. Draw an improved version of the warning and describe why you feel it is a more usable than the prior warning. Feel free to reference your analysis in the prior question (a) or use other frameworks such as NEAT and SPRUCE.

A.1 Example Answer

1. The answer should cover all the main elements of how people process warnings. The modifying elements such as "Personal Variables" are typically used in the context of the warning processing to justify or explain likely user action.

   Communication Impediments: The communication appears to be a full screen warning which blocks the whole web browser. Therefore most users will be able to physically see it without occlusion or environmental distractions.

   Communication Delivery: Attention switch is forced here, since the full screen is taken up. Attention maintenance is more challenging, the warning looks like an error so the user may not progress past the big text at the top and may simply hit "Try again" or try it using a different browser or device. Knowledge and Experience may play a role here too if the user has prior experience with computer errors or this type of warning, they are less likely to maintain attention. Attitudes and Beliefs may also modify Attention Maintenance, if the user has the attitude that they never understand these errors, or that they have no self-efficacy around their ability to handle "technical problems".

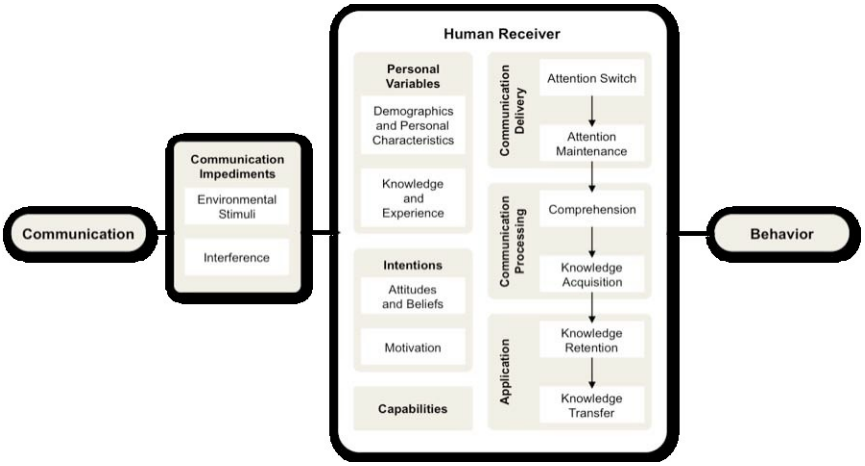


Figure 1: Framework for Reasoning about the Human In The Loop.

Communication Processing: Comprehension is a serious issue here, terms like "Diffie-Hellman key" are not readily understandable to the general population. Typical Internet users are unlikely to be able to comprehend what has happened. Knowledge Acquisition is similarly impeded. The error gives no ability to learn more about what caused it and running a Google search of the terms is likely to end the user on a Wikipedia article about how Diffie-Hellman key exchange works mathematically, which is unhelpful. The user will likely find it difficult to learn what to do about the error, and the provided guidance of contacting the website administrator to report the error will likely not be within the user's Capabilities as it requires a complex sequence of steps.

This stage is also likely to be heavily impacted by Motivation. User motivation to understand browser errors is not high and therefore they are likely to give up quickly. If they really want to reach this page they are likely to ignore the warning and simply try a different way of accessing it, not understanding the risks. On a more positive side, their low motivation may also cause them to do the safe thing and stop trying to access the site if getting through proves too difficult.

Application Knowledge Retention refers to the user's ability to remember knowledge they have learned previously such as the meaning of terms or icons and Knowledge Transfer refers to their ability to identify situations where that knowledge could be applied and apply it correctly.

The presented warning is problematic for both areas. This type of warning is rare, most people will never see it at all. Hence Knowledge Retention is unlikely to occur as it requires that the user encounter terms regularly or in a highly memorable way. Most users will have never seen these terms and are unlikely to have retained them from prior experience.

If the user happened to be a highly trained person familiar with these terms (say a computer security student) knowledge transfer would only really be useful if they also had the Capability to contact the system administrator. This type of error means that either the server has a serious server-side error, or the NSA is actively attacking the connection. In both cases a user has no hope of solving the situation client-side.

Behavior: The warning author likely had three possible behaviors in mind when they wrote the warning: 1) Reload the page and hope that something weird happened with the connection on the first attempt. 2) Contact the website owner to get them to fix their server settings. 3) Realize there is a security issue and stop trying to access the website.

Considering the above analysis, most users will have no trouble with the first behavior, even

someone who has trouble with Attention Maintenance, will find the "Try Again" button and click it. However, if doing so will not solve the problem the second behavior is unlikely unless the user is the system administrator or someone else who is both highly trained and motivated. The third behavior is likely to happen by accident for unmotivated users, though they are unlikely to realize that their is a security issue here at all.

2. An improved warning would follow the SPRUCE guidance to help a user understand what has happened and put the issue in their language. It would also target the issues identified in the above analysis.

   Below is a rough sketch of an improved warning dialog.

   Secure Connection Failure

   The website you are trying to communicate with does not support modern security approaches for encryption. If you proceed to this site your information will not be guarenteed to be secure and could be read and modified by other people.

   What can I do?
   It is recommended that you try the following:
   1. Reload the page - Sometimes this error happens due to a temporary communication problem with the site.
      [Try Again]
   2. Search for this site on Google - You may have the wrong page and Google can help you find the correct one.
      [Google Search Box]
   3. Contact the website owner - They may have a problem that they do not know about. Until they correct the problem it is not safe to use this page.

   [More details]