

FIA session III.4 – Security and Usability

Rapporteurs/Organisers: Nick Papanikolaou (HP Labs, UK – np1@hp.com), Fabio Massacci (University of Trento - Fabio.Massacci@unitn.it)

Other contributors: Jim Clarke (TSSG – Waterford Institute of Technology – jclarke@tssg.org)

Session summary

This session was highly successful, and clearly brought to the fore several important issues and concerns that need to be addressed in order to balance the often conflicting needs for a usable and secure Future Internet.

The talk by Corrado Leita discussed, with extensive use of examples, two potential approaches to helping users to be safe online, and highlighted their pitfalls. First, there was the idea of educating users to be safe and to use e.g. antivirus and firewall software; examples were given of social engineering attacks and dialog boxes imitating genuine antivirus warnings which work all too well in fooling an ‘educated’ user. The second approach, of building disruptive security software which presents a series of warnings to users, can also be unhelpful, as warnings are all too easily ignored. The speaker concluded emphasizing that finding the right compromise is a difficult challenge.

Angela Sasse discussed numerous attempts to design helpful authentication mechanisms for users, giving several examples of real systems and highlighting the problems that emerge in practice as user behavior is often unexpected (e.g. users choosing pictures of faces arbitrarily or in a very biased way from a set of pictures intended for entry into a system). The speaker emphasized that effort required on the part of the user is the key factor in designing successful systems. In addition, security researchers were told to ‘get real’ with regard to usability and that mechanisms that require too much time or effort to use have either low compliance, or a high cost of enforcement.

Kai Rannenberg discussed the PICOS project, which developed user interfaces for mobile devices, enabling users to configure privacy settings. Frank Stajano identified a number of common tricks fraudsters use to deceive users, and how these apply in the online world. In particular, the speaker identified seven key principles that are used, and these are documented in a recent paper. The final speaker, Florian Mansmann, discussed visual analytics, and showed how graphical representations can help to understand security threats and the spread of attacks in diverse environments.

The discussions focused on whether the research communities are examining the generational (age) requirements of security, privacy and usability, how things may get worse before better in this topic and being able to push the users as well as technology is pushed is necessary and will require significant inputs from the technology, psychology and usability domains for it to be successful as a next step.

Links and info

FIA programme: <http://fi-budapest.eu/download/SDIII4.pdf>

Speakers and links to their presentations:

| | |
|----------------------|--------------------------------|
| Dr Corrado Leita | link to slides |
| Prof Angela Sasse | link to slides |
| Prof Kai Rannenberg | link to slides |
| Prof Frank Stajano | N/A |
| Dr Florian Mansmann: | link to slides |

Questions and discussion

One of interesting thing is the lack of transparency. User cannot understand what is good choice and bad choice. If they choose no, things don't work. They can't distinguish between browsing without protection on or off. Is there some way you can make this transparent to the users?

Answers:

- KR: you can visualise to the user – established culture and tradition to visualise this. For abstract concepts, there are metaphors that can be used. For anglers, they used the sub- communities ideas and the users were then able to understand based on pre-understood concepts.
- Metaphors are strong elements here – some people say you should fight metaphors as they could make misunderstanding but this was found not to be the case in the PICOS trials.
- Someone else made a comment that Metaphors can work, not work, or can cause abstractions to be imprecise.
- Symantec : It is unfair to say things haven't improved in making more transparent. Some effort have been made to highlight these aspects to the user today. For example, two years ago, there was a small lock icon saying it was locked. Now they have green bars to say you are safe.
- The face remains if you try to stop a user from doing something, this will make the user try to do something as a work-around. Eg. downloading bit torrent file, the user might try to circumvent the blocks.
- Lot of knowledge about design but they are not taking advantage of usability design. One of links is action to actual interface. If you have two buttons that look the same, the user won't be able to tell the difference.
- From an engineering viewpoint, if model only makes sense to people who made it, the users won't be able to use it correctly.
- Metaphors don't translate that easily as other concepts in computer science.

Comment: fault is happening in technology – lot of security services were not adopted because they did not understand them. A study was done with users for privacy awareness but it is improving but still a long way off of where it should be. Angela Sasse says you need to go back to the beginning to the requirements. Some experts from IBM from long ago claim the functionality of devices are used only 20% . Has any study been done on usability, how it has been developed and what users are accepting or developing.

Is this is more designed for our generation or the next generation? Watching children now they don't trust it the way that we expect children are using fictitious accounts for Skype etc. Will this apply to children?

Answers/discussion:

- KR: Agree with experience from anglers perspective. There were younger anglers and older anglers.
- Some young people are more aware of privacy issues more than engineers. Regarding usability,
- Partial identity is part of the solution. We present a different face to each other dependent on our

(Nick W): Is this one of these things that we cannot solve? A question for all panellists: Are there solutions out there? Is it going to improve over the next 10 years.

- It will get worse first before it gets better? The community hasn't got it what the user wants. Until this message is received and understood, it is going to get worse. It is nice to see people discussing it but it will be a while before it gets better. It is not a universally spread urge and until it percolates through, it will get worse.
- KR: There are a lot of things that can be understood eg. credit card fraud. If someone asks for one technical solution, it won't get better,. We are on a journey there and we collect a number of possible tools and evaluate them. Prudent decisions can be made and we can avoid big mistakes like in the past. Often now we discuss smaller disasters.
- New generations are learning about the situation. Other problem that cannot be answered, if you treat people like children, they will act like children. And if you don't involve them, they won't take a role. But then others don't want to know the details.
- A good approach is to start with assumption that we will fail. Try to find ways to deal with them. Putting more security in the development processes. Google Chrome is an example with security design since the beginning. By trying to tolerate our failures and adding mechanisms, we can have an approach to attack this.
- We are good at pushing our systems to the limit but we are not good at pushing the users to the limit. Have a powerful capability of establishing models out of random data points, users are very capable. Lot of work on psychology and usability domain that hasn't been addressed.