Usable Security Tool for Investigative Journalists

Aneesh Dasari

Master's Thesis
Master in Interaction Design
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College,

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Usable Security Tool for Investigative Journalists

Aneesh Dasari

2012/07/15

Abstract

Investigative Journalists have been playing a pivotal role in unearthing lot of hidden truths buried under the carpets. They have been instrumental in exposing incompetence, corruption, lies, abuse of power and broken promises etc. In the process of communicating with sources and collecting, analyzing, investigation, disseminating of information, the Interactive tools play a role of catalyst in performance of their job. J.D.Tygar and A Whitten most renowned researchers have identified a “weakest link property". The property states that stating that muckrakers can exploit when users make error while using the digital tools.

Therefore a single error made by investigative journalists while using digital tools may lead to loose data and there will be a chance for muckrakers to find out their sources identity. This research is oriented towards the study, evaluation and improving usability of security tools by considering mental model of the investigative journalists. There are many digital security tools currently available for investigative journalists like Tor browser, Text Secure, Red Text and so on for protecting their data and sources. But the tools mentioned above faces usability issues by which users may tend to stop using the tool gradually or may tend to make errors. Most of the security tools available in the market are developed for larger audience and not specifically for investigative journalists and according to Pew research centre many investigative journalists don’t use digital security tools to protect their digital privacy because there more chance for loosing the data and they can be traced by geo-location and so on.

Therefore, in this thesis I will design an application by considering the investigative journalist requirements. Furthermore, the tool will be designed in such a way that both investigative journalists who are technically sound and those are who aren’t; are comfortable in operating/using is also emphasised. Improvisation of usability tools and enabling all the Investigative Journalists to enjoy the fruits of technological breakthroughs, emerging out of day-to-day research work by consolidation and orientation towards employing cognitive walkthroughs, interviews, usability testing.

Preface

I would like to thank Cristina

Contents

List of Figures

List of Tables

1 Introduction

It is broadly acknwoledged that security tools are only effective when they are used by all the end users, who are technically savvy and those who aren't. Technically well implemented code will not provide security if users are unable to use the primary features of the tool. Human errors are one of the main reason for most of the security system failures. However, still the user interfaces or the features of the security tool are designed to be clumsy and confusing. Therefore, this research will focus on the need to improve the usability for security tools which are used by investigative journalists like Tor, Cryptocat, TextSecure and so on [2]. The reasons for the security system failures are assessed by evaluating the existing tools.

1.1 Keywords

Privacy, anonymity, investigative journalist, usability.

1.2 Problem description

"There is a usability gap that is transformed directly into usage gap", if users don't know how to use the security tool even with appropriate awareness [3]. However, this gap may force the end user to stop using the tool or to mis-use the key security features like encryption, public keys, private keys, signatures and so on. Generally, security tools provide privacy and anonymity for the end-users and also protects information from their adversaries. Moreover, privacy and anonymity depends on the set of users using the tools. Larger the set, higher the anonymity and privacy are achieved [4]. For suppose if the number of users stops using the security tool which provides anonymity and privacy, then privacy levels get decreased for the existing user. In order to increase privacy and anonymity levels for both existing user and new user. The tool should be designed in a way that it can be used by users, who are technologically savvy and also by those who are not. Then, there may be a chance for more numbers users to use the security tool [5]. Therefore, usability affects the security in systems that aim to protect data confidentiality. But when the goal is privacy, it becomes even more important [4].

There are some secured tools like Tor Browser, RedPhone, TextSecure, Cryptocat and so on, which are highly recommended for investigative journalists to protect the data and identity of the sources [2]. Tor browser avoids someone viewing your web history and provides access to sites that are blocked [1]. RedPhone and TextSecure has the capability to secure the exchange of conversations made from their personal mobile phone/smart phones and provide end to end encryption. Chat and Text messages are safe and cannot be decoded even if the phone is lost [2]. Cryptocat provides encrypted chat in browser and mobile phone[3]. These tools are technically well implemented, but they are haunted by usability issues like a frequent crash of web pages, missing

[1] https://www.torproject.org
[2] https://whispersystems.org
[3] https://crypto.cat

translations and extraction issues for Tor browser [6]. Connectivity issue within the interfaces due to various configuration for different devices and issues like no feedback to the user is provided when the problem is raised for RedPhone [7]. Duplication of contacts in the contact list and some issues with the color interface design and feedback to the user for TextSecure [8]. Usability issues due to language differences and lack of cultural integration for Cryptocat [9].

Investigative journalists spend months or years to verify in-depth truths, discover hidden secrets, shed a spotlight on social justice and accountability, that may involve crime, corruption and corporate wrongdoing etc. During investigating or researching on any social issue, international or any other issues, investigative journalists contact their source and colleagues, located across the globe. [10] They are highly protective about their data and contacts because adversaries may try to mislead the investigations or threaten investigative journalists; their colleagues and sources. The usability issues that are described above may prevent the investigative journalists to use the features that are essential. These issues may also lead to misuse of features with out the knowledge of investigative journalists. Which results in creating a risk for them, their sources, data and colleagues. At present, It is broadly acknowledged that security requirements can't be addressed by technical means alone, and the chances of success will be essentially affected by the users involved [3]. Therefore, this research will coherently evaluate current existing tools that are used by investigative journalists, explore the challenges of usable security, prevailing problems and propose a usable interactive solution based on observations.

1.3 Justification, motivation and benefits

The assessment and improvement of security tools in terms of usability are important for investigative journalists to maintain high privacy and anonymity levels. But if improved, it helps in minimize the human and interface errors that would occur while using the security tools [3]. Chances of risk get decearsed and provides support for investigative journalists to discover hidden truths and perform investigations with regard to social justice.

Many of the previous works have expressed and showed how important it is to improve usability in secure system tools, like in the work done by J.D.Tygar et al [11]. Evaluating the security tool PGP 5.0 to know whether is it usable and produce effective security of most computer users. After evaluating the PGP 5.0 tool, they have observed that desipte of it's attractive computer interface, it is not usable for most its computer users [11].

The identified problem when solved can be very beneficial for investigative journalists during situations like discovery of truths about government officials (who otherwise are powerful people and any slackness in maintaining secrecy at investigation stage will be hazardous and may obliterate the whole exercise), investigating about a bank robbery or about any issue when they are accountable for public etc. The soluble will help the investigative journalists to maintain confidentiality of the information and identity of the source from their adversaries.

1.4 Research questions

The research questions included in this work are:

1. How are the existing secured tools used by investigative journalists are user friendly?

2. How does the existing tools provide a dependable amount of privacy and anonymity while maintaining usability?
3. If privacy and anonymity are comprised due to design flaws in terms of usability, then how can it be fixed?

1.5 Planned contributions

In this research the problem addressed above can be solved by considering the previous best resulted works [11] [12]. In this work a more structured and precise steps will be implemented by considering most useful factors to find a better solution to the problem. The work from [11] [12] [3] [4] [9] [13] are extracted and organized to formulate a new methodology to provide a more improved solution to the problem addressed.

2 Usability

"*The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use*" -The definition of usability according to ISO 9241 standard

3 Literature Review

First section will give an overview of previous related works and the major contributions regarding usable security are described in this section. Second section illustrates Human computer interaction- security guidelines and third section describes readical shift and impact of technology on investigative journalists.

3.1 Usable Security

The concept of usable security was first instigated in 1975 by Saltzer and Schroder [14]. In their work they have derived design principles for protection of information in security systems and identified the need of physchological acceptability in system that do security operations. The psychological acceptability is defined as “It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user’s mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors [15]". This statement provides a platform for programmers to design the interfaces by considering the user mental model. Mental model is A mental model is the “representation that a person has in his mind about the object he is interacting with" [16].

The work of J.D.Tygar and A Whitten [11] has influenced most of the programmers and researchers to consider user requirements while designing the security mechanisms and their paper “Why Jhonny can’t encrypt" is widely cited in most of the research works [12] [4] [3] [13] [17]. Sometimes the errors made by the users may lead to security failures therefore J.D.Tygar and A Whitten have argued that effective security requires a different usability standard and that is not achieved by using user interface techniques that are applied for designing other softwares. They have defined usability for security as "Security software is usable if the people who are expected to use it:"

1. are reliably made aware of the security taks they need to perform;
2. are able to figure out how to successfully perform those tasks;
3. don’t make dangerous errors;
4. are sufficiently comfortable with the interface to continue using it. [11]

They have also identified five problematic properties of security for user interface design:

1. **The unmotivated user property**: The general tendency of the people who use computers is that the information is secured till such time the area of work and use of computer is kept secluded. Most of the users feel that the information is always secured and are busy in sending emails, download software’s and browse web pages. Many users are not concerned

of the security measures and are of the apprehension that everything is secured and risk free since they have secluded the working area and therefore only concentrate on their work devoid of security measures. Therefore, the designers of Interface Security cannot be under the impression that the user will go through manuals and look for the security tools that are designed to be self-effacing. It is also evident that application of security measures in case found cumbersome or unfriendly there is always a tendency of the users avoiding and in search of alternatives.

2. **The abstraction property**: Grant of accesses to resources depends on security policies which are systematic and based on abstract rules which are the main criteria to provide accessibility rights. Programmers while designing such rules makes them as a general task and the same may not be in the knowledge of the general user population. Therefore, while making the User Interface design for security the programmers need keep this in mind.
3. **The lack of feedback property**: The system of feedback helps in improvisation of the software and also prevents the possibility of most rectifiable errors and some time prevents serious errors. However, providing feedback by the users for security management is complex and varies from user to user. The requirements of the user mainly caters by the correct security configuration and only the user will be aware of the requirements, therefore it is difficult for the software to perform the check of errors.
4. **The barn door property**: Even by mistake any time even for a short duration a secret is left insecure there is no guarantee that the same has not fallen into the hands of the attacker. Therefore, to avoid such incidents the user interface design for security needs to accord top priority in ensuring that the user is made aware and avoid is making such security mistakes may be sometimes they are too costly.
5. **The weakest link property**: Even the minutest mistake by the user may give the advantage to the cracker and may be some times end the game. Therefore, the use needs to be made aware of the security in all aspects. [11]

To test the hypothesis mentioned above, they have looked for existing software that has good user interface design for security. Therefore they have selected PGP 5.0 for Macintosh as its user interface has appeared to be resonably well designed by general consumer standards [11]. They have set minimum usability standard that PGP 5.0 need to meet to enable people to successfully use it to secure their mail. They have selected two methods to evaluate security tool PGP 5.0: informal cognitive walk-through and usability testing. Cognitive walk-through is a usability evaluation method where a series of tasks and set of question are asked from the perspective of user [18, p.84] and it mainly tends to focus the learnability of the user interface for the users who are technically savvy and for those who are not [11]. They have evaluated the visual metaphors, encryption key types, key management policy, key server and irreversible actions of PGP 5.0 tool. As the results drawn from cognitive walk-through mostly rely on the evaluators [18, p.84]. To get best results the evaluators should have better knowledge about the user interfaces, therefore J.D.Tygar and A Whitten had conducted usability test to achieve better results. Usability testing is conducted by performing experimental tasks with real users and it helps in finding usability

problems before writing any code. Therefore they have designed the test to check whether the PGP 5.0 meets the required usability standards. J.D.Tygar and A Whitten have given a scenario to the participants to do security tasks. After performing both the evaluation methods, they have noted usability problems in PGP 5.0 tool. But the tool is well acknowledged for its design as their marketing literature has stated that " It has improved graphical user interface makes complex mathematical cryptography accessible for novice computer users." [11]

Jeremy clark et al. [12]have worked on a privacy tool Tor, that provides anonymous web browsing capabilities. They have evaluated four competiting methods of deploying Tor clients, and number of software tools that have intergrated Tor: vidalia, Privoxy, Torbutton, FoxyProxy and TorPark. They have used cognitive walk-through, which is suggested by J.D Tygar et al to evaluate the tools. They have also considered the usability standard guidelines proposed by J.D.Tygar et al [11]. Their aim behind using the cognitive walk through is that users learn by exploring the software interface rather reading the software or user manuals. Due to time and cost constraints they have not performed any usability tests. For conducting cognitive walk-through they have designed core tasks and evaluator will do these taks and evaluate the usability of the application against set of evaluation guidelines which are drawn from [19] [11] [20] [21] [22], the guidelines used are mainly intended for Tor specifically and the guidelines are: [12]

1. Users should be aware of the steps they have to perform to complete a core task.
2. Users should be able to determine how to perform these steps.
3. Users should know when they have successfully completed a core task.
4. Users should be able to recognize, diagnose, and recover from non-critical errors.
5. Users should not make dangerous errors from which they cannot recover.
6. Users should be comfortable with the terminology used in any interface dialogues or documentation.
7. Users should be sufficiently comfortable with the interface to continue using it.
8. Users should be aware of the application's status at all times. [12]

In the work, Challenges of understanding and using security: A survey of end users, S.M.Furnell et al [3] had scrutinize the possible usability challenges in security features of end-user softwares. They mainly considered software packages like Windows XP, Internet Explorer, Word and Outlook Express. They have outlined key points that will influence overall usability of the resulting protection [3].

1. **Understandable** – Options and descriptions should be presented in a manner that is meaningful to the intended user population. Security offers a great deal of potential for the use of technical terminology and other jargon, but this could easily come at the cost of excluding a proportion of the users. Sufficient help and support should be available to assist novices to achieve the level of security that they need.
2. **Locatable** – Users need to be able to find the features they need. If casual users have to

spend too long looking for security, it increases the chances that they will give up and remain unprotected.

3. **Visible** – The system should give a clear indication of whether security is being applied. Appropriate use of status indicators and warnings will help to remind users in cases where they may have forgotten to enable appropriate safeguards.

4. **Convenient** – Although visibility is important, the provision of security should not become so prominent that it is considered inconvenient or intrusive. Users are likely to disable features that become too much of an impediment to legitimate use. [3]

They have conducted a survey to assess end-user understanding of security features in common software applications. The researchers [3] have felt that respondents would feel more comfortable and interested in answering the questions about programs they were familiar with. Therefore they have selected above tools as they are well known and widely used. They haven't use cognitive walk through or the usability test because survey findings offer a revealing insight into difficulties that may lay users are likely to experience when attempting to understand and use the security aspects of the software placed before them. Total of 342 responses are recorded during the survey period. The questionnaire began by asking whether the users are aware of security feautures in software packages mentioned above. The survey findings have identified that most of the users could not able to understand or dont know the security features of the mentioned packages. For example in regard to the security features related to Microsoft outlook express the findings revealed that 65 percent of the respondents did not understand the meaning of digital ID and 61 percent of the respondents did not understand the use of term encrypt. Based on the findings of survey conducted on widely used software packages portray that security features should be designed in a way that most of its users should understand in using it. S.M.Furnell et al [3] has suggested that default settings of the security features of an application should provide sufficient protection for majority of users using the application [3].

3.2 Guidelines

Katsabas.D, et al. [13] in their work used number of Human computer interaction applied in area of security and had evaluated three anti-virus applications: Norton Antivirus, Panda Antivirus,Agnitums Outpost Firewall, Zone Alarm Firewall, McAfee Virus Scan, as well as Opera and Mozilla Firefox web browsers, Qualcomm's Eudora, Incredimail email client software and finally Microsoft Word. These applications are evaluated by conducting usability test and evaluated according to the level of attention that they afforded to have key issues. The software tool Mozilla Firefox obtained relatively low score, as it did not satisfy most of Human computer interaction guidelines that applied in security area. Most of the guidelines are drawn from Johnston et al [23] work and other guidelines are created by modifying 10 usability heuristics proposed by Nielsen. They have proposed ten guidelines and the applications mentioned above are evaluated against each one of them. [13]

1. **Visible system state and security functions**: The users are not expected to search for security tools or find hidden security tools hidden inside the application. The users are always kept aware and informed about the state of system by the use of status mechanisms and

therefore the status information should be automatically updated and easily accessible.

2. **Security should be easily used**: The security settings should not be scattered at different places and interface should be so designed that the user may utilize the security features with less effort and easily accessible.
3. **Suitable for advanced as well as first time users**. The application of security should be designed in such a manner that even the first timer can use it easily and the information so provided should not be lengthy that the advanced user also can refresh. To better the usage of software more easily and quickly shortcuts may be provided.
4. **Avoid heavy use of technical vocabulary or advanced terms**: It is always better to use simple language and avoid technical vocabulary and advanced terms so that it is easy for the beginners to apply the security features.
5. **Handle errors appropriately**:Application needs to be planned cautiously in such a manner that errors which occur while making use of security measures can be prevented or minimized as much as possible. Pop ups of error messages should be evocative and problem solving.
6. **Allow customization without risk to be trapped**: Default values should be easily and automatically restored by providing exit paths when by mistake some wrong functions are chosen.
7. **Easy to setup security settings**: Enabling easy to setup security settings will make the user more confident and help in changing and configuring the application need based.
8. **Suitable Help and documentation for the available security**: To assist the users when they face difficulties, suitable help and documentation should be provided to ease out and overcome the problems.
9. **Make the user feel protected**: The application needs to assure the users that their work is totally protected. Application should make sure that the users do lose the data when unexpected errors are made and the recovery of data is easy without any loss. Latest security features should be incorporated so that the user feels highly protected.
10. **Security should not reduce performance**: Application of security features should be so designed by applying efficient algorithms so that there is smallest amount of impact on the effectiveness of the application. [13]

3.3 Technological impact on investigative journalists

In this section the problems faced by investigative journalists due to technology are discussed as it's already said in the above section that it is important to know the mental model of investigative journalists for minimizing the rate of occurence of errors. Firstly, the technological changes are being discussed and followed by the postives of technological shift are discussed. Then problems arised due to radical change in technology are discussed.

Investigative reporting was developed during the 18th century, mainly in France, England and American colonies. In the early years of 19th century it was admired by public for its accountability and social justice and by the end of world war II the traditional approaches/techniques like

interviews, tracking public documents and so on are well understood by the practioners. [24] During 1980's, world with the emergence of high-speed technology like internet [25], personal computer, video cassette recorder [26] and so on, changed the traditional journalism into digital journalism with the emergence of new tools and practices that are redefining the place of journalism. This change is called as Journalism 2.0 by researchers and journalists [27]. The fusion of computer power and news reporting sometimes called computational journalism" [28]. According to Hamilton and Turner (2009) [29] computational journalism supplement the accountability functions of journalism by bringing algorithms, data and social science together. Diakopoulos et al. (2010) [30] suggest that computational journalism helps journalists in doing their work, such as by providing visualization tools and filtering source information. According to Lewis and Usher (2013) [31] many scholars argued that computational journalism will lead to better investigative journalism and new forms of engagement are created with end-users or audience.

(Steensen (2011) [32], in their research work have measured the success rate of online journalism based on interactivity, multimedia and hypertext and these are called as technological assets. Hypertextuality is about linking and layering of digital information through a hierarchial structure. interactivity is all about engaging user participation in the process of information seeking and sharing and the use of more than one type of media in a single device or product [32]. They have also stated that these technological assets have a greater impact on online journalism, which is also called as digital journalism. Kawamoto (2003) [25] has defined digital journalism as "The use of digital technologies to research, produce, and deliver news and information to an increasingly computer-literature audience." [25] have drafted the characteristics that are typical online journalism: Hypertext, customization, convergence, personalization and nonlinearity to the technological assets. They have also stated in their work that if there is a change in technology then the concept of journalism changes and the definition of digital journalism also changes.

The technological advancements/breakthroughs like internet, email service, voice and video chat etc., helps the reporters to have direct contacts with their editors and contacts all over the globe. The greater use of data analysis, web software by journalists, computer scientists and citizens has incommensurate increased in the recent past. In this advanced environment where the journalists at present work, new realities are uncovered every day, audience feedback is integrated; more differing viewpoints on the same stories are consistently introduced; more stories are accessible and searchable [33]. Mosco (2004) [34] argues that "the entry of new technologies has always been surrounded by Myths about their revolutionary power" like an iPod which made stronger impact on the growth of technologies. Entry of new technologies have always been revolutionary, create enormous power and surrounded by myths about their capabilities. The rise of machines (computers and their software) and networks have played major role in creating future for investigative journalism.

These factors mean more focus to the investigative journalism itself, more citizen involvement in shaping stories, and more collaboration. As Knight foundation encourages [35] - investigative

journalism itself focus on involvement of more citizens in shaping stories resulting in more collaboration than competition. In fact, the past few years have seen remarkable growth in non-profit newsrooms and greater use of data analysis and Web software by groups composed of journalists, computer scientists, and citizens. These initiatives then use new technology to create networks of newsrooms to share information, to improve the quality of their investigations, and to create cost efficiencies. It is no exaggeration to state that the new technologies have transformed the practices of investigative journalists all over the world and Norway has not been an exception. “As Norway was among the first countries to connect to the internet and according to the Jupiter research, Norway is one of the most digitally advanced markets in Europe" [36]. The impact of new technologies on investigative journalism has revealed dialectical impact and suggests that the Internet, email and cellular phone play a pivotal role in enhancing the results in reporting. These gadgets have strengthened the Journalists in meeting their day-to-day requirements of collection, investigation and interaction which are the main elements in cracking the stories and bringing the truth out.

Alan Rusbridger has stated that “All journalism is investigative to a greater or lesser extent, but investigative journalism it is a bit of a tautology is that because it requires more, it’s where the investigative element is more pronounced." [37, p.17] Therefore, the effect of technology on journalism also implies to the investigative journalism. According to Franco (2009) [38] the impact of digital technology on journalism occur in three principal categories.

1. The dynamics of news and information generation
2. Professional practices and skills that are necessary in digitized environment
3. Situation of traditional media.

There are several databases like Government websites, News organization databases and other nonprofit organization databases (Hate speech International Norway, Icelandic Centre for Investigative Journalism Iceland, the Norwegian Foundation for Investigative Journalism (SKUP)) available for investigative reporters to get access to or to retrieve the documents that are important for journalists to do in-depth research. [39]. Computer Assisted reporting helps the journalists to store the procured data into a software like google spreadsheets, Microsoft excel sheets or other statistical packages for analysing the information. Both databases and Computer assisted reporting provides an overview of the story, which is being researched by the journalist. There are a number of methods and tools already available for retrieving the documents from the massive database for journalists, some of them are google fusion tables, google public data explorer, google refine etc. [24]

Ottosen and Krumsvik (2012) [36], in their research work, have reflected the survey conducted by Norwegian union of journalists in 2007 among 715[1] journalists in digital media. The findings show that majority of the journalists who have participated in the survey believed that digitization of the work environment help in maintaining positive relationships with their col-

[1] Sample includes all members of the Norwegian Union of Journalists working on digital and multimedia platforms

leagues, improves the relationship with management and they felt comfortable when the digital platform is introduced but some of them claimed that they are worse off than before. The participants also suggested some valuable suggestions for a better journalism. The suggestions include, better conditions for investigative reporting, opportunity to specialize and to do more in-depth work in their own stories, more discussions in the newsrooms. But in a survey conducted by Pew research center [1] fifty percent of investigative journalists said that their organizations are not providing enough resources to protect their identity, data and sources from adversaries. Fourty seven percent of them said that their respective organization are providing valuable digital protection resources. In this survey, 671 investigative journalists consisted editors, producers, photo journalists etc, responded to online survey. All the respondents of survey are members of Investigative Reporters and Editors, Inc. (IRE) [1].

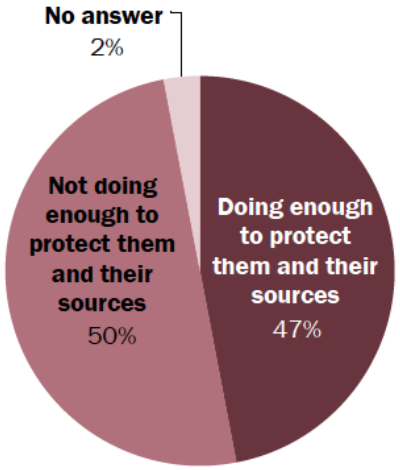

Figure 1: Investigative journalists respond on resources provided by their orgnizations, Pew research center [1].

The internet has become a new tool or source for investigative journalists [39]. Internet offers accessible sources for journalists to research or investigate. Some of them are Non-government organizations, official government sources, Databases, Computer Assisted Reporting (CAR) etc, the one thing that the journalists resources can do for reporters to make reporting easier. Presently, most of the governments all over the world have gone online. The policy documents, responsibilities, data, press release, materials, etc. related to government institutions are included in the government official websites. Thus, it is easier for the journalists to search for relevant documents, when required to research on any issue. According to the survey conducted by Pew Research Center [1], only two percent of the investigative journalists have a lot of confidence on Internet service providers(ISP's). Seventy one percent of the respondents doesn't have confidence on Internet service providers(ISP's), shown in figure 2. The reason for not depending on ISP's due to digital threats like surveillance and hacking. [1]

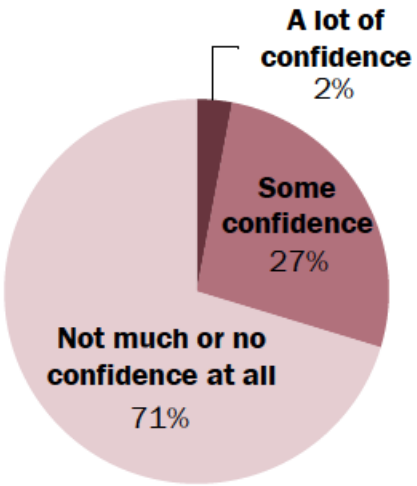

Figure 2: Level of confidence on Internet Service Providers, Pew research center [1].

Most of the news organizations, investigative journalists and other journalists came to know more about surveillance systems when Edward Snowden [40]revealed about the PRISM surveillance system of the United States of America. Most prominent U.S technological companies like Google, Apple, Microsoft etc provide information to Prism system through National security agency(NSA) to keep surveillance on specific people. Journalists comprising of different fileds came to realize that every electronic communication like email, messaging, phone calls and so on are being recorded, stored and analyzed [40]. These advances are obtained by government institutions to keep an eye on their public and press. According to the survey conducted by Pew Research Center [1], most of the investigative journalists in United states of America feel that their government has already collected their data(phone call or online communication), figure 3. Therefore, Investigative journalists are more worried about protecting the identity of sources and the data (contact information, the story data, facts and so on) [2]. Investigative journalism is a high risk profession and some times investigative journalists are targeted even if he/she is not working on sensitive story because their colleagues may work on sensitive stories. Then adversaries may target the respective journalists in order to dig into the issue [40].

There are other surveillance systems like Prism that are operated by some government institutions to track the data. Iran utilizing a surveillance system[2] that is developed by Nokia-Siemans Networks, Libya uses a system developed by Amesys and other companies[3] (French company) ,

[2]http://news.bbc.co.uk/2/hi/technology/8112550.stm
[3]http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle

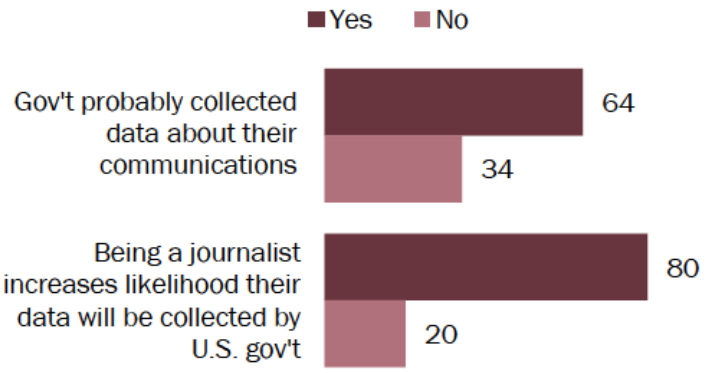

Figure 3: Data collected by U.S government, Pew research center [1].

Unite States of America uses a surveillance system called PRISM[4] maintained by National Security Agency (NSA). Due to these type of digital threats most of them have started using digital tools like TextSecure for secure online chat, RedPhone for a secured phone communication, Tor for anonymous web browsing and many. According to the survey conducted by Pew Research Center [1](figure 4), 14 percent of respondents revealed that they have stoped contacting their sources due to surviellance systems and three percent of them had stoped covering the senstive stories. Half of the respondents have changed their way of storing/sharing sensitive documents and 38 percent of respondents have changed their way of communication to contact their sources.

Most of the investigative journalists started using secured digital tools to store documents, to

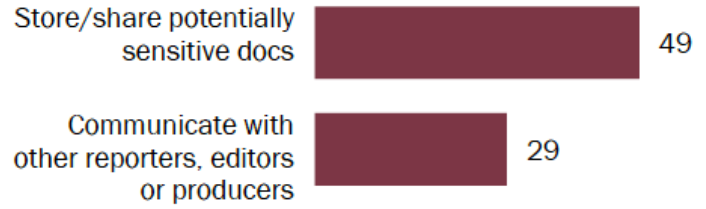

Figure 4: Changing ways to collet data and to communicate with adversaries, Pew research center [1].

communicate with their colleagues or sources. After snowden disclosure about the surviellance system at United States of America(U.S.A), most of the investigative journalists are afraid to rely on digital tools beacuse most of the tools are geo located and adversaries can easily locate them at a faster rate. According to the survey(PEW Research center) [1] nearlly half of the respondents(figure 5) are not using any one of the tools that are classfied in survey. The survey researchers have included tools from email encryption to turning off geolocation on mobile devices [1]. Description about tools are not revelead in survey because of security issues.

[4]www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline

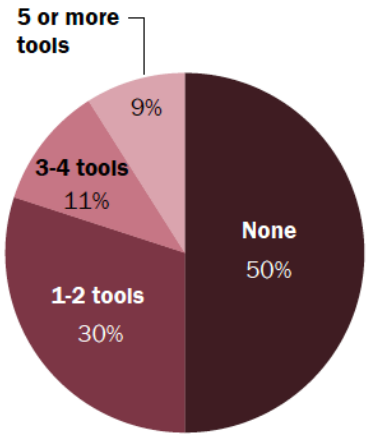

Figure 5: Use of digital secured tools by investigative journalists according to Pew research center [1].

3.4 Digital tools

4 Methods

Research methods are classified in to two types 1) Qualitative Method and 2)Quantitative Method [41]. In our research, we are implementing the Qualitative method. To address the first and second research question, we will perform a case study on three existing tools described in 1.2: Cryptocat, TextSecure and RedPhone. The case studies in human computer interaction(HCI) have four goals: [41]

1. **Exploration**: Understanding the problems or situations, often with the hopes of informing new design.
2. **Explanation**: Developing models that can be used to understand a context of technology.
3. **Description**: documenting a system, a context of technology use, or the process that lead to proposed design.
4. **Demonstration**: Showing how a new tool is sucessfully used. [41]

Therefore, the case studies helps us in understanding the problems faced by investigatice journalists while using the digital security tools and it will also help in developing a process based on the results. There are four components of a case study design: research questions; hypothesis or propositions; units of analysis;data analysis plan. Research questions describes the goals of thesis and hypothesis or propositions are the statemetns of what you expect to find. The unit of analysis determines the focus group and finally data analysis plan is helpful in planning the data collection. [41] The research questions are mentioned above in section 1.4and 1.2. The unit of analysis is a group of investigative journalists and in this research work the data analysis plan start firstly by employing cognitive walkthrough method to evaluate the digital security tools mention in section 1.2, as it has been used previously by the researchers mentioned in section 3. Cognitive walkthroughs are often very good at identifying certain classes of problems, especially showing how easy or difficult a system is to learn or explore effectively – how difficult it will be to start using that system without reading the documentation, and how many false moves will be made in the meantime. [22]

In cognitive walkthrough, set of core tasks are developed and these tasks are designated differently for the three digital security tool mention above. We will perform these tasks and evaluate the usability of three security tools: Cryptocat, TextSecure and RedPhone against set of guidelines. These guide lines are to be derived from the previous works [11] [12] [13] [3]. To address the third reseach question, although the results from the cognitive walkthrough may provide valuable information regard to the problems faced in existing tools. In this research we will also use contextual inquiry to draw the user requirements. It is one of the best methods to understand the users' work context and it is basically a structured field interviewing method.

Contextual inquiry is more a discovery process than an evaluative process; more like learning than testing. This technique is best used in the early stages of development, to gain and understand how people feel about their jobs; how they carry out their work; how information flows through the organisation, etc. [42] According to [43] stated that “The best results come from testing no more than 5 users" because at the best they provide better results. Therefore, contextual inquiry for this research work, we will test no more than 5 users. Based on the results from cognitive walkthrough and contextual inquiry, we will develope a paper portotype.

After developing a paper prototype, we will use the method card sorting, it helps in understand the investigative journalists expectations. Card sorting is a method The card sorting helps in designing the information architecture according to user needs. By conducting card sorting, there is a chance for getting more insights from the users. [44] Then by considering results that are dervied from card sorting, cognitive walkthroughs and contextual enquiry, we will design the high fidelity prototype. Prototype which is close to the final product. Then perform a usablity testing for evaluating high fidelity prototype, as it produces more objective results. A usability test is conducted to draw the usability problems and this method is conducted mostly in earlier stages or the final stages of the designing process. For conducting the usablity test we will design a real test scenario and ask the users to use the prototype in realtion to scenario.

Bibliography

[1] Amy M, Jesse H, K. P. 2015. *Investigative journalists and digital security: Perception of Vulnerability and Changes in Behavior. PewResearchCenter*. PewResearch Center.

[2] Williams, M. March 2014. Beginner's guide to improving online security. `www.icij.org/blog/2014/03/beginners-guide-improving-online-security`.

[3] Furnell, S. M., Jusoh, A., & Katsabas, D. 2006. The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1), 27–35.

[4] Dingledine, R. & Mathewson, N. 2006. Anonymity loves company: Usability and the network effect. In *WEIS*.

[5] Pfitzmann, A. & Köhntopp, M. 2001. Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing privacy enhancing technologies*, 1–9. Springer.

[6] Mikeperry. June 2013. Usability|announcing tor browser bundle 3.0alpha1. `https://blog.torproject.org/category/tags/usability`.

[7] WhisperSystems/RedPhone. July 2014. Registration failure leaves user stuck (usability issue). `https://github.com/WhisperSystems/RedPhone/issues/183`.

[8] WhisperSystems/TextSecure. February 2014. Improve usability / look of contacts list. `https://github.com/WhisperSystems/TextSecure/issues/741`.

[9] Kobeissi, N. & Breault, A. 2013. Cryptocat: Adopting accessibility and ease of use as security properties. *arXiv preprint arXiv:1306.5156*.

[10] Looney, M. January 2013. Four things investigative journalism is not. `www.ijnet.org/en/blog/four-things-investigative-journalism-not`.

[11] Whitten, A. & Tygar, J. D. 1999. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Usenix Security*, volume 1999.

[12] Clark, J., Van Oorschot, P. C., & Adams, C. 2007. Usability of anonymous web browsing: an examination of tor interfaces and deployability. In *Proceedings of the 3rd symposium on Usable privacy and security*, 41–51. ACM.

[13] Katsabas, D., Furnell, S., & Dowland, P. 2005. Using human computer interaction principles to promote usable security.

[14] Sasse, M. A. & Flechais, I. 2005. Usable security: Why do we need it? how do we get it?

[15] Saltzer, J. H. & Schroeder, M. D. 1975. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278–1308.

[16] Weinschenk, S. 2011. *100 things every designer needs to know about people*. Pearson Education.

[17] Brodie, C., Karat, C.-M., Karat, J., & Feng, J. 2005. Usable security and privacy: a case study of developing privacy management tools. In *Proceedings of the 2005 symposium on Usable privacy and security*, 35–43. ACM.

[18] Baecker, R. M. 2014. *Readings in Human-Computer Interaction: toward the year 2000*. Morgan Kaufmann.

[19] Chiasson, S., van Oorschot, P. C., & Biddle, R. 2006. A usability study and critique of two password managers. In *Usenix Security*, volume 6.

[20] Karat, C.-M., Brodie, C., & Karat, J. 2005. Usability design and evaluation for privacy and security solutions. *Security and Usability*, 47–74.

[21] Reagle, J. & Cranor, L. F. 1999. The platform for privacy preferences. *Communications of the ACM*, 42(2), 48–55.

[22] Wharton, C., Rieman, J., Lewis, C., & Polson, P. 1994. The cognitive walkthrough method: A practitioner's guide. In *Usability inspection methods*, 105–140. John Wiley & Sons, Inc.

[23] Johnston, J., Eloff, J. H., & Labuschagne, L. 2003. Security and human computer interfaces. *Computers & Security*, 22(8), 675–684.

[24] DeFleur, M. H. 2013. *Computer-assisted investigative reporting: development and methodology*. Routledge.

[25] Kawamoto, K. 2003. *Digital journalism: Emerging media and the changing horizons of journalism*. Rowman & Littlefield Publishers.

[26] Oxford, T. 2009. 8 technologies to thank the 1980s for. `http://www.techradar.com/news/world-of-tech/8-technologies-to-thank-the-1980s-for-635764`.

[27] Kaul, V. 2013. Journalism in the age of digital technology. *Online Journal of Communication & Media Technologies*, 3(1).

[28] Flew, T., Spurgeon, C., Daniel, A., & Swift, A. 2012. The promise of computational journalism. *Journalism Practice*, 6(2), 157–171.

[29] Hamilton, J. T. & Turner, F. 2009. Accountability through algorithm: developing the field of computational journalism. In *A Center for Advanced Study in the Behavioral Sciences Summer Workshop. Duke University in association with Stanford University*, 27–31.

[30] Diakopoulos, N., Naaman, M., & Kivran-Swaine, F. 2010. Diamonds in the rough: Social media visual analytics for journalistic inquiry. In *Visual Analytics Science and Technology (VAST), 2010 IEEE Symposium on*, 115–122. IEEE.

[31] Lewis, S. C. & Usher, N. 2013. Open source and journalism: toward new frameworks for imagining news innovation. *Media, Culture & Society*, 35(5), 602–619.

[32] Steensen, S. 2011. Online journalism and the promises of new technology: a critical review and look ahead. *Journalism Studies*, 12(3), 311–327.

[33] Van der Haak, B., Parks, M., & Castells, M. 2012. The future of journalism: Networked journalism. *International Journal of Communication*, 6, 16.

[34] Mosco, V. 2004. *The digital sublime: Myth, power, and cyberspace*. MIT Press.

[35] Media.illinois.edu. 2014. Illinois college of media public service knight chair. `http://www.media.illinois.edu/knight/knight-foundation-support-of-investigative-reporti`.

[36] Ottosen, R. & Krumsvik, A. H. 2012. Digital challenges on the norwegian media scene. *Nordicom Review*, 33(2), 43–55.

[37] De Burgh, H. 2008. *Investigative journalism*. Routledge.

[38] Franco, G. 2009. The impact of diital technology on journalism and democracy in latin america and the caribbean.

[39] Knight, A. 2001. Online investigative journalism. *Retrieved May*, 25, 2011.

[40] Silkie Carlo, A. K. November 2014. *Information Security for Journalists; Protecting your story, your source and yourself online*. `http://www.tcij.org/node/1016`.

[41] Lazar, J., Feng, J. H., & Hochheiser, H. 2010. *Research methods in human-computer interaction*. John Wiley & Sons.

[42] Holtzblatt, K. 2014. Contextual design. *The Encyclopedia of Human-Computer Interaction, 2nd Ed.* `https://www.interaction-design.org/encyclopedia/contextual_design.html`.

[43] NIELSEN, J. 2014. Why you only need to test with 5 users. `http://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/`.

[44] Hudson, W. 2014. Card sorting. *The Encyclopedia of Human-Computer Interaction, 2nd Ed.* `https://www.interaction-design.org/encyclopedia/card_sorting.html`.