Foundations of Computer Security

Homework Assignment 1

Divay Prakash
2014039

Ans 1)

Experiment 1 : Find out the voter I-card number of staff of IIIT Delhi, using Electoral Search. This method does not require any other information other than the name of the person, resulting in very easy access to sensitive information namely the EPIC number, polling station and father's name. I was able to find the same for Professor Pankaj Jalote and Professor PK.

Experiment 2 : Find out the PAN card details of IIT staff, using Search PAN. This method requires entering the name and DOB of the person. The DOB can be retrieved in a variety of ways, such as

- using the calendar provided on the ERP portal
- using Google calendar by searching through email addresses on the IIIT directory
- using social accounts such as FB, LinkedIn etc. to find out birth date and month, and estimating year of birth from CV by checking year of graduation

Ans 2A)

Study to measure the strength of passwords

Collection :

Passwords can be collected from a variety of sources, some of them being :

- Password dumps by black-hat hackers
- Password dumps from security researchers and analysts, one such example being a large collection of 10 million passwords released by security consultant Mark Burnett, through his site http://xato.net
- Passwords collected by a survey of people and offering them a chocolate to just suggest a password that they might use for any of their various accounts, or provide their actual password(s)

Analysis :

I would use the following criteria to measure the strength of passwords in a study:

- Password should not be a variation of the information already provided by user, such as name, initials etc.

- Password should not contain any dictionary words or continuous pattern such as **1234**, **abcd** etc.
- Whether the password is pronounceable or not, and accordingly how easy it is to memorise
- Password should contain a mix of uppercase and lowercase letters, numbers and special characters

The analysis could be created to assign a score (say, on a scale of 1 through 10) to each password as a measure of its entropy(E) ie. the degree of randomness. The 'guessability'(G) of the password can then be quantified as the inverse of the entropy, that is $G = 1/E$.

Ans 2B)

Good practices to follow while creating a password :

- Password should not be a variation of the user's information such as name, DOB, address etc.
- It should not contain any continuous patterns, such as **1234**, **abcd** etc. and also should not contain any repetition, such as **blahblah**, **123random123** etc.
- Password should not be a keyboard sequence, such as **qwertyuiop**, **fghjkl** etc.
- Password should be of a minimum length of 8 characters
- Password should be pronounceable but not a dictionary word, which provides security as well as insures that it is easy to remember
- Password should contain a mix of letters, numbers and special characters

Ans 2C)

People can be encouraged to follow these practices in the following ways :

- Use of password meters to provide users a graphical, easy-to-understand representation of the 'strength' of their chosen password
- Informing users of the risks they are at by an unsuitable password choice
- Periodical reminders and deadlines to change password
- Not allowing reuse of an old password

Ans 3A)

Privacy policy for Enki, which can be found here.

OECD principles :

- Collection limitation :
    - *Among the types of Personal Data that this Application collects, by itself or through third parties, there are: Cookies, Usage data, first name, last name, company name, profession, email address and username*

    - *Other Personal Data collected may be described in other sections of this privacy policy or by dedicated explanation text contextually with the Data collection*
- Purpose specification :
    - *The Data concerning the User is collected to allow the Owner to provide its services, as well as for the following purposes: Analytics, Contacting the User, Content commenting, Hosting and backend infrastructure and Managing contacts and sending messages*
    - *The User's Personal Data may be used for legal purposes by the Data Controller, in Court or in the stages leading to possible legal action arising from improper use of this Application or the related services*
- Security safeguards :
    - *The Data Controller processes the Data of Users in a proper manner and shall take appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data*
- Individual participation :
    - *Users have the right, at any time, to know whether their Personal Data has been stored and can consult the Data Controller to learn about their contents and origin, to verify their accuracy or to ask for them to be supplemented, cancelled, updated or corrected, or for their transformation into anonymous format or to block any data held in violation of the law, as well as to oppose their treatment for any and all legitimate reasons. Requests should be sent to the Data Controller at the contact information set out above*

FTC principles :

- Notice and disclosure :
    - *Among the types of Personal Data that this Application collects, by itself or through third parties, there are: Cookies, Usage data, first name, last name, company name, profession, email address and username*
    - *Other Personal Data collected may be described in other sections of this privacy policy or by dedicated explanation text contextually with the Data collection.*
    - *The Personal Data may be freely provided by the User, or collected automatically when using this Application*
    - *Any use of Cookies - or of other tracking tools - by this Application or by the owners of third party services used by this Application, unless stated otherwise, serves to identify Users and remember their preferences, for the sole purpose of providing the service required by the User*
    - *Users are responsible for any Personal Data of third parties obtained, published or shared through this Application and confirm that they have the third party's consent to provide the Data to the Owner*

    - *The Data processing is carried out using computers and/or IT enabled tools, following organizational procedures and modes strictly related to the purposes indicated. In addition to the Data Controller, in some cases, the Data may be accessible to certain types of persons in charge, involved with the operation of the site (administration, sales, marketing, legal, system administration) or external parties (such as third party technical service providers, mail carriers, hosting providers, IT companies, communications agencies) appointed, if necessary, as Data Processors by the Owner. The updated list of these parties may be requested from the Data Controller at any time*
    - *The Data concerning the User is collected to allow the Owner to provide its services, as well as for the following purposes: Analytics, Contacting the User, Content commenting, Hosting and backend infrastructure and Managing contacts and sending messages*
    - *The User's Personal Data may be used for legal purposes by the Data Controller, in Court or in the stages leading to possible legal action arising from improper use of this Application or the related services*
- Data quality and access
    - *Users have the right, at any time, to know whether their Personal Data has been stored and can consult the Data Controller to learn about their contents and origin, to verify their accuracy or to ask for them to be supplemented, cancelled, updated or corrected, or for their transformation into anonymous format or to block any data held in violation of the law, as well as to oppose their treatment for any and all legitimate reasons. Requests should be sent to the Data Controller at the contact information set out above*
- Data security
    - *The Data Controller processes the Data of Users in a proper manner and shall take appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data*

Ans 3B)

Comparative study of privacy policies of 3 different organisations, namely Flipkart, Newegg and NCIX, according to OECD principles :

- Collection limitation
    - All three websites collect personal information of the user such as name, address, telephone, email address, credit card/debit card/other payment instrument details etc. Also, Flipkart specifies that it collects the URL the user came from and the one to which he/she navigates next, as well as '***automatically*** *track certain information about you based upon your behaviour*'. Newegg and NCIX have similar statements in their policies too.

Additionally, all three websites specify that '*By visiting this Website you agree to be bound by the terms and conditions of this Privacy Policy. If you **do not agree** please **do not use or access** our Website. By **mere use** of the Website, you expressly consent to our use and disclosure of your personal information in accordance with this Privacy Policy.'* This is quoted from the Flipkart policy, however Newegg and NCIX are similar, all three breaking the principle of collection limitation in the process

- Data quality
    - The information stored by all websites is relevant to the purposes for which it is to be used
- Purpose specification
    - All websites clearly specify the uses of the collected user data
- Use limitation
    - There are issues with this principle in all the policies
        - Flipkart
            - '*In our efforts to continually improve our product and service offerings, we **collect and analyse demographic and profile data** about our users' activity on our Website. We identify and use your IP address to help diagnose problems with our server, and to **administer our Website**. Your IP address is also used to help identify you and to gather broad demographic information*'
        - NCIX
            - '*We may also **analyze and act upon your personal and account information** as part of our standard business practices. We occasionally purchase from third parties commercial information such as company size, number of employees and annual sales of other companies. We may use this commercial information along with your personal and account information to customize our offerings to you, as well as for our **internal use***'
        - Newegg
            - '*We will, however, **link data stored in cookies to the personally identifiable information** you submitted while on our site. This allows us to personalize your shopping experience and discern user preferences to evoke subconscious feelings of familiarity and assurance*'
    - Flipkart and Newegg also specify sharing information with their partners, however while Newegg explicitly states that '*(third parties) have **limited access** to your personal information and **may not use** it for other purposes*', Flipkart doesn't, breaking the use limitation principle

- Security safeguards
    - All websites state that personal data is protected by various security safeguards, with Newegg being very verbose and detailed whereas NCIX and especially Flipkart just skim over this section
- Openness
    - While Newegg states that it provides various means of notifying users about changes in the privacy policy, Flipkart and NCIX do not, merely stating that it is the user's prerogative to check the privacy policy page to review any changes
        - Flipkart
            - '*If we decide to change our privacy policy, we will post those changes **on this page** so that you are always aware of what information we collect, how we use it, and under what circumstances we disclose it*'
        - NCIX
            - '*NCIX.com reserves the right to modify this privacy policy from time to time. You should **visit our Web site** periodically to review any changes*'
        - Newegg
            - '*If we decide to change our Privacy Policy, we will post those changes to this **privacy statement**, the **homepage**, and **other places** we deem appropriate so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. We reserve the right to modify this privacy statement at any time, so please review it frequently. If we make material changes to this policy, we will notify you **here**, by **email**, or by means of a **notice on our homepage**. If you have opted out of receiving communications from Newegg.com, you will still be able to view news of policy changes at www.newegg.com. Otherwise, you may **e-mail us** at webmaster@newegg.com or **call us** toll free at (800) 390-1119 to ask our customer service department about changes and updates*'
- Individual participation
    - Newegg specifies that '*Customers may change or review their stored account information such as street address or e-mail address through our website by visiting our Help section*', however NCIX and Flipkart do not state anything in this regard, having no process for individual participation at all
- Accountability
    - Neither of the three websites make any statements in this regard

Ans 3C)
Privacy policy for my organisation :

- Data collected : We collect your name, account number, address, telephone number, email address, credit card/debit card/other payment instrument details, and additionally, information from cookies such as browser type, login information and purchase/browsing history, referral web site, navigation information and IP address
- Purpose specification and use limitation : The data collected is used to personalize your shopping experience, as well as provide you services such as order delivery, customer service and for marketing purposes. It is also used to conduct internal research on our users' demographics, interests, and behaviour to better understand and serve you. Your data may also be shared with our partners in order to provide you access to our services, and also to fulfill any legal obligations. The amount of personal information shared in such a manner is kept to a minimum, with third parties not allowed to use the data for any purposes other than those specified
- Data quality : The data collected is processed to ensure accuracy and completeness
- Security safeguards : We employ stringent security measures in order to protect your information. Our website is HTTPS compliant and uses SSL encryption to transfer any sensitive data. Our website and data servers are housed in a secure facility and highly protected against unauthorised access
- Openness : In case of any changes to this policy, all users will be notified via email as well as banners on the website homepage
- Individual participation : In case of any issues, you may contact us to modify/delete your personal information at the contact details provided
- Accountability : In all cases, our organization and partners are not liable for any damage/loss that is unforeseeable
- Company name and address

Ans 4A)
Similarity between Vigenere and Caesar cipher : Both ciphers use simple shifts to encrypt cleartext.
Difference : While Vigenere cipher is polyalphabetic, Caesar cipher is monoalphabetic. Accordingly, the Vigenere cipher is much more difficult to break due to its resistance to frequency analysis. The Caesar cipher encrypts cleartext by simple left/right shifts and thus does not change the frequency distribution, which can be used to crack the encryption and determine shift value. However, depending on key length, Vigenere

ciphers are much stronger being a combination of multiple Caesar ciphers and immune to frequency analysis.

Ans 4B)
The Feistel cipher is a is a symmetric structure used in the construction of block ciphers. It is completed over multiple iterations, using a round function.

Ans 5)
The guards at IIIT Delhi allow anyone to enter the college premise without a IIITD ID card as long as they enter their details in a ledger. This practice while being very usable is highly insecure. Any person needs to only enter some unverified details (which could very well be fake) in the ledger to gain access to IIITD. Thereafter there is no check to verify identity.

An alternate system for entering the college is using RFID chips in IIITD ID cards, thus requiring the ID cards to be placed on a scanner to verify identity and allow access to the campus, similar to the entry/exit system in the Delhi metro. In case of delivery men/visitors etc., a log could be created on the ID card of the person within IIITD to ensure security.

This system is very usable, not requiring much effort on the part of the users. However, care would have to be taken in case of exigent circumstances, such as procedures to follow in case somebody forgets his/her ID card and to allow guardians of students access using logging facility on the student's ID.

The system could be improved by logging the in/out times of students and not allowing two consecutive entries/exits to ensure security. Further, facial recognition could be carried out using cameras at the entrances to match the person entering to the ID card he/she is using.

*****