Security in Computing

Reinventing eIDs

Arno De Witte, Kwinten Pardon

Todo list

1 In-depth Analysis of the Problem Statement and Protocols

The current way the Belgian Electronic identity card (eID nowadays works makes it hard to implement the use of the Belgian eID in commercial activity due to some privacy concerns. The Belgian eID releases the the user's name and national registry number at each authentication which makes you uniquely identifiable. This makes sense when we look at the eID from a government instances where you need them to be identifiable. Think about healthcare and the need to store your medical history as well as law enforcement when receiving a ticket for speeding.

However, when we take 3rd party applications into account, the release of these attributes becomes a clear issue. When releasing sensitive, uniquely identifiable, information about one self leaves them viable for identity theft. it also allows companies to create data stores where the record the purchase history of each of their customers. This might be useful to the companies to create personal advertisements based on their history. This information has become valuable as personalised advertisement has gain in popularity. However, This information is released at every authentication which causes the customers to be unable to opt out. If the use of the Belgian eID by 3rd party applications were to become widespread, they would be able to create detailed profiles of their customers. This information could cause harm when fallen in the wrong hands.

For this reason, an alternative system has been implemented with the focus on safeguarding the user's privacy.

2 Evaluation

- **What elements are lacking in order to commercialize the system as an alternative for the current eID cards?**

Think about it, .. I have no clue at the moment

- **How can you build a certificate chain? What is verified during authentication?**

just explain how certificates work?

- **Storing a common private key on each eID card implies a substantial risk. What risk? How can you mitigate the risk?**
  When the private key is stolen in an attack, one may create an eID card for any identity he likes. This is because only the private key is required to determine the validity of the card and the private key is shared among all citizens.

Find other vulnerabilities. Elaborate on this vulnerability.

- **How is the authentication of the SP to the card realized in the protocol?**

explain step 2 in words I guess?

- **How can stolen eID cards be revoked? How can the server check the revocation status of eID cards?**
  By changing the key pair (SK_{CO} - PK_{CO}) and issuing the new public keu PK_{CO} to the *Service Providers*, All eID cards would be revoked. This is because all eIDs share the same (SK_{CO} - PK_{CO}) key pair. The authentication of the card is accomplished by the *Service Provider* sending a challenge using the previously established symmetric key. The card decrypts the challenge and signs it with SK_{CO} The sign and $Cert_{CO}$ are then encrypted using the same symmetric key and send back to the server. The server will decrypt the message again and check the sign using PK_{CO}. If the key pair has changed, the validation will fail because the card used the old SK_{CO} to sign the challenge. This method is however only a defensible solution when SK_{CO} has been stolen. revoking all cards over the theft of one seems to be overkill.

Find method that works on a single card or at least a smaller set

- **How can server certificates be revoked? How can the revocation status of server certificates be checked on the card?**
  We could expand the Government Server to include a certificate revocation list storing the certificates that have been revoked. When the card is in the process of authenticating the certificate, he first send the certificate to

the Government Server who will look up the certificate in the certificate revocation list. If present, the authentication of the *Service Provider* will fail.

- **How can you transfer the data of the current Belgian eID card securely to the new eID card? Can the government mediate in this process?**
  The Belgian eID expires every five year, forcing the owner to renew his identity card. The way the renewal if your eID works is that your local city hall informs you when your new eID is available at to be retrieved. This means that the government already transfers the data to a new card at five year intervals. When a new eID systems would be taken into use, the government could mediate this process by simply handing over the new type eID upon renewal. This process could be sped up by forcing the population to renew their eID more quickly.

- **Give a short performance analysis. What is the authentication time of the new eID? Is this acceptable? What are possible bottlenecks?**

  Arno? What is the authentication time?

- **Assume that no secure random generator is available on the smart card. How to set up a secure communication channel?**
  The *Service Provider* authenticates to the card by sending its certificate. The card will initiate the handshake in order to create a secure communication channel when the certificate is valid. If the card would not have a any way of creating a random number, the card could reply with a message to the Service provider to inform him that he is allowed to initiate the handshake. Alternatively, the *Service Provider* could initiate the handshake and send this information along with the certificate upon authenticating. When the card successfully authenticates the *Service Provider* he solves the challenge and replies with the new challenge to complete the handshake.

- **How to prevent that malicious service providers can steal data on the card?**

  isn't that done by issuing certificates allowing access to only a set of attributes? Check this

- **Are Man-in-the Middle attacks possible? Why (not)? Make a clear analysis.**

  examine architecture in detail

- **Compare the Belgian eID card to the alternative eID card. Give a table with differences related to security and privacy.**

  lecture 5