Blind Signatures

CSC 335
Presentation by Genevieve Heydt

The Purpose and Usage of Blind Signatures

- To be able to certify that messages came from a valid source, without giving away the specific source they came from
- Common uses
  - Votes, secure elections, feedback surveys
  - Anytime you want to collect information but only from select individuals who have been authenticated, without attaching their details to the information collected

How is this done?

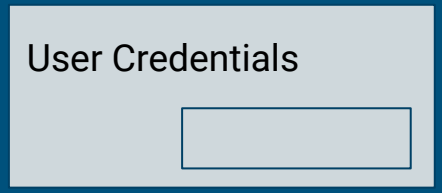
Physical Blind Signatures

- Use Carbon Transfer Paper
- 4 steps

1. User's credentials are preprinted on a carbon lined envelope
2. Message is written, then enclosed in the carbon paper lined envelope
3. An official verifies the credentials, then signs the envelope
    a. This puts only the verifier's signature on the original message document
4. Package is passed back to the original user who removes the envelope and places the document in a new, blank envelope

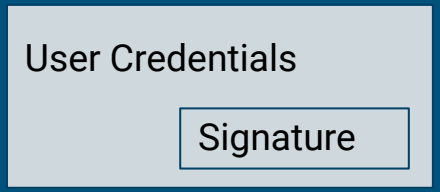
Physical Blind Signatures Continued

Step 1:



Step 2:

Step 4:



Step 3:

How does this translate to cryptographic Blind Signatures?

(Digital Blind Signatures)

Cryptographic Blind Signatures

- Different from other digital signatures because of its blindness
- The signer (certifier) is unable to link a valid message-signature pair
- Requester (user) chooses some random factors and embeds them in message to be signed
- Signer cannot recover message because of the secret random factors
- Once returned, the requester can remove the random factor to obtain a valid signature

Lin et.al's Blind Signature Scheme: Signer Joining System

1. Signer A with identity ID_A chooses a number x as her partial private key
   a. Corresponding public key is computed: $P_A=xP$
2. A sends (ID_A, P_A) to the trusted system authority SA
3. SA computes partial private key d_A using master key s
   a. Where H(X) is a cryptographic hash function
   b. $d_A = sH(ID_A||P_A)$
4. This is returned to A

Lin et.al's Blind Signature Scheme: Signing a Message

1. Signer A and User B establish common information Δ to get signature on message m
2. Signer chooses a random number r and computes
   a. R'=rP
   b. S'=rH($ID_A||P_A$)
3. Signer sends (R',S') to B
4. B randomly chooses three numbers α,β,γ to compute
   a. R=αR'+γ(P_{pub}+P_A)
   b. S=αS'+$\alpha\beta$H($ID_A||P_A$)-γH(Δ)
   c. h=α^(-1)H(m,R,S)+β
5. Then sends h to A
6. Signer A computes and sends ξ to B
   a. ξ=(h+r)(xH($ID_A||P_A$)+d_A)+rH(Δ)
7. User B unbinds ξ as $\varsigma=\alpha\xi$
8. Message m now has blind signature (S,R,ς)

Lin et.al's Blind Signature Scheme: Verification

A signature (S,R,ς) is only valid if

$e(\varsigma,P) = e(S+H(m,R,S)H(IDA||PA),Ppub+PA)e(H(\Delta),R)$

Purpose and Uses of Digital Blind Signatures

- General Purpose: Confirm messages/ data comes from valid user while keeping information anonymous
- Examples
  - Anonymous voting
  - Anonymous feedback
  - Digital Cash transactions
  - Anywhere in which related privacy protocols would be useful

Are Digital Blind Signatures Secure?

Attack on Lin et.al's Blind Signature Scheme

1. Suppose an adversary produces a forged signature on message m in the name of identity ID_i, the attack is as follows:
   a. Randomly choose r and set public key of the identity as $P_i=rP-P_{pub}$
   b. Then randomly choose k and compute R=kP
   c. Randomly choose S and compute $\varsigma=r(S+H(m,R,S)H(ID_i||P_i))+kH(\Delta)$
   d. The forged signature on message m is (R,S,ς)
2. The signature is valid because:
   a. $e(\varsigma,P)= e(r(S+H(m,R,S)H(ID_i||P_i)),P)$
   b. $e(\varsigma,P)= e(S+H(m,R,S)H(ID_i||P_i),rP)e(H(\Delta),kPe(H(\Delta),R)$
   c. $e(\varsigma,P)= e(S+H(m,R,S)H(ID_i||P_i),P_{pub}+P_i)e(H(\Delta),R)$

Why is this attack valid?

- This attack is valid because the signature is valid
- The public key identity of ID is free, not fixed
- To overcome this attack, there must be a limit on the form of the user's public key P_{ID}

Expectations

- There are challenges to Blind Signatures
  - It’s hard to think about how things can go wrong when you’re focused on requirements
- Blind Signatures are an important concept that if fully secured, could open a lot of possibilities
- More applications will open up in the future

Sources

Chaum D. (1984) Blind Signature System. In: Chaum D. (eds) Advances in Cryptology. Springer, Boston, MA. https://doi.org/10.1007/978-1-4684-4730-9_14

Islam, S.H., Amin, R., Biswas, G.P. *et al.* Provably Secure Pairing-Free Identity-Based Partially Blind Signature Scheme and Its Application in Online E-cash System. *Arab J Sci Eng* 41, 3163–3176 (2016). https://doi-org.libproxy.umflint.edu/10.1007/s13369-016-2115-5

J. Zhang and S. Gao, "Cryptoanalysis of a Self-Certified Partially Blind Signature and a Proxy Blind Signature," 2009 WASE International Conference on Information Engineering, 2009, pp. 184-187, doi: 10.1109/ICIE.2009.141.

Yeu-Pong Lai and Chin-Chen Chang, "A simple forward secure blind signature scheme based on master keys and blind signatures," 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers), 2005, pp. 139-144 vol.2, doi: 10.1109/AINA.2005.63.