Towards Practical Anonymous Password Authentication

Yanjiang Yang, Jianying Zhou, Jun Wen Wong, Feng Bao

Institute for Infocomm Research
Singapore
Agenda

• Introduction
• Limits of Conventional Anonymous Password Authentication
• Our Approach in ACSAC’09
• Addressing Membership Withdrawal & Online Guessing Attacks
• Conclusion
• Introduction
• Limits of Conventional Anonymous Password Authentication
• Our Approach in ACSAC’09
• Addressing Membership Withdrawal & Online Guessing Attacks
• Conclusion
PA: Pros & Cons

• Password Authentication (PA)
  – Most widely used entity authentication technique
  – Advantages: portability
  – Disadvantages: guessing attack
    • Online guessing attack
    • Offline guessing attack
Privacy Concern

• Privacy is increasingly a concern nowadays

• Password authentication in its original form does not protect user privacy
PA: Standard Setting

User (PW\textsubscript{i})

Server

Password File

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>U1</td>
<td>PW1</td>
</tr>
<tr>
<td>U2</td>
<td>PW2</td>
</tr>
<tr>
<td>U3</td>
<td>PW3</td>
</tr>
</tbody>
</table>

Ui, PW\textsubscript{i}

Un, PW\textsubscript{n}
Privacy Protection – Anonymous PA

- Unlinkability

Server

| U1, PW1 |
| U2, PW2 |
| U3, PW3 |

Unlinkability

Ui, PWi

Un, PWN
• Introduction
• Limits of Conventional Anonymous Password Authentication
• Our Approach in ACSAC’09
• Addressing Membership Withdrawal & Online Guessing Attacks
• Conclusion
Major Weakness

• **Server Computation** $O(N)$
  – Linear to the total number of registered users $N$
  – Server is the bottleneck of the system
• Introduction
• Limits of Conventional Anonymous Password Authentication
• Our Approach in ACSAC’09
• Addressing Membership Withdrawal & Online Guessing Attacks
• Conclusion
A Different Setting

User

- pw
- Password-protected credential

Credential

Server

- secret key
- Password File
  - U1, PW1
  - U2, PW2
  - U3, PW3
A Different Setting - Cont

User

PW

Server

secret key

Portability ← Server Efficiency

IMPORTANT: [cred]PW is public, requiring no further protection

[cred]PW
Design Rationale

- *cred* must be shown anonymously
- Limited Verifiability of *cred*
  - *cred* must not be publicly verifiable; otherwise, everyone can guess PW from *[cred]PW*
  - *cred* is verifiable only to server
Instantiation

• *cred* must be shown anonymously
  – A credential is defined to be a CL signature (Camenisch and Lysyanskaya)

• Limited verifiability of *cred*
  – The server is assumed to have a public key encryption, and part of a credential is encrypted under the public key
Limitations

• Due to the use of CL signature and Paillier encryption, computation is heavy.

• It has no support of membership withdrawal.

• It does not consider online guessing attacks.
• Introduction
• Limits of Conventional Anonymous Password Authentication
• Our Approach in ACSAC’09
• Addressing Membership Withdrawal & Online Guessing Attacks
• Conclusion
Overview of Contributions

• Heavy computation
  – Use BBS signature (Boneh, Boyen, and Shacham) → CL signature
  – ElGamal encryption → Paillier encryption

• Membership withdrawal
  – Dynamic accumulator

• Online guessing attacks
  – Virtual TTP: users and server together act as TTP
Basic Scheme

• A user u’s credential is \((M, k, u, s)\) s.t. 
  \(M=(a^u b^s d)^{1/(k+x)}\), where \(a, b, d\) are 
  public parameters and \(x\) is the secret 
  key of the BBS signature

• \([cred]PW = \{u, [M, k]_{PW}, E(s)\}\)

• To show the credential:
  – Recover \(M, K\) using \(pw\)
  – Select \(r\) and randomize \(E(s)\) to be \(E(r.s)\)
Basic Scheme - cont

- The basic scheme is comparable to the scheme in ACSAC'09, but with much better efficiency.
- Denote the zero-knowledge proof as $\text{ZK}[(M', k, u, s', r) : \text{R-BBS}]$.
- It lacks support of membership withdrawal.
- Not consider online guessing attacks.
Support of Membership Withdrawal

• Use of the **Accumulator** technique
• The server publishes an accumulator \( acc \), which accumulates all valid \( k \)
• Each valid user is issued a witness \( wit \) showing that her \( k \) is contained in \( acc \)
• \( \text{ZK}[(M', k, u', s', r, wit) : (R-BBS) \land (k \in acc)] \)
Online Guessing Attacks

• Online guessing attack is inherent, due to the low entropy of passwords
• In regular password authentication, system-level measures, e.g., freezing a victim user’s account, are effective
• However, it becomes particularly troublesome in anonymous password authentication
Possible Solutions

• All-Or-Nothing method
  – Once attacks occur, freeze all users’ accounts

• Short-term credentials
  – Each credential has a expiry time.
  – How to determine the validity period is difficult

• TTP-based anonymity revocation
  – A TTP helps revoke user anonymity
  – TTP has public key encryption $E_{TTP}(.)$
Virtual TTP

- Also submit $E = E_{TTP}(k)$ and $\mathbf{ZK}[(M', k, u', s', r, wit) : (R - BBS) \land (k \in acc) \land E = E_{TTP}(k)]$

• Our final solution – virtual TTP

  - Server and users form a virtual TTP, together can revoke user anonymity
  - The server alone cannot revoke user anonymity
  - Even if all users collude, they cannot revoke user anonymity
Virtual TTP - cont

• The key issue is how to generate the public key of vTTP
  – There is no trusted “dealer” that helps distribute shares of the private key to the share holders
  – The private key should not be reconstructed on any entity at any time

• Dynamic threshold cryptosystems fulfil these properties, and we can use ElGamal-type of them
Virtual TTP - cont

\[ PK_{vTTP} = PK_{Server} \]

\[ PK_U = g^{xS+XU} \]
Experiments Results

• We implemented a prototype of our scheme, and particularly to test the actual efficiency.
• Programs were written in C++ and utilized Miracl library for elliptic curves and pairing operations.
• Use DDH-hard subgroups of an MNT elliptic curve with pairings, where \(|q| = 159\) bits, and the curve has an embedding degree of 6.
Experiments Results - cont

• Client program runs on a Fujitsu notebook, Intel Core2 Duo CPU, 2.53GHz; Server program runs on a PC, Dell Dimension 9150, Intel 3.0 GHz CPU, 1GB RAM

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>User</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>385</td>
<td>430</td>
</tr>
</tbody>
</table>
• Introduction
• Limits of Conventional Anonymous Password Authentication
• Our Approach in ACSAC’09
• Addressing Membership Withdrawal & Online Guessing Attacks
• Conclusion
Conclusion

• Server computation in conventional anonymous PA has to be $O(N)$

• We proposed new approach in ACSAC’09 achieving constant server computation, but has not considered membership withdrawal and online guessing attacks
Conclusion - cont

• Addressing online guessing attacks in anonymous PA turns out to be challenging

• We solved the above two issues, by using different types of primitives, and our new scheme has better efficiency

• Implementation results showed that our scheme demonstrate acceptable performance
Q & A

THANK YOU!