Ensemble Approach to Failure-Resistant Password-Based Key Derivation Functions

Jason Hennessey, Sarah Scheffler, Mayank Varia

{henn, sscheff, varia}@bu.edu

Motivation

- PBKDF2 [3] (most widespread PBKDF) relies on simple, repeated hash invocations to increase password key derivation time for attackers
- Bitcoin provided a financial incentive to create high throughput, efficient hashing ASICs
- Passwords can now be guessed $10^6$ to $10^{10}$ times faster using ASICs than CPUs of similar price
- State-of-the-art PBKDFs (e.g. scrypt [8], argon2d [4]) improve by utilizing memory, but are still vulnerable to ASIC attacks [1]

Goal

Minimize efficiency gains of specialized hardware vs. honest user’s device for key derivation

Properties

- **Resource consumption model** - plugins consume user-specified resources (e.g., memory, CPU, disk)
- **Failure resistance** - Hash construct guarantees security as good as strongest hash; failures in resource-consuming plugins limited to a single round
- **Optimization for specific platform** - Plugin and sponge construction designed for anti-pipelining and anti-parallelism

Acknowledgements

We gratefully acknowledge Ethan Holman’s contributions to the initial concept and subsequent, as well as earlier research from NSF Grant No. 1116124, NSF Grant No. 1514764, and Open Cloud.

Construction

PBKDF Definition

```
password
salt
key length
key
```

Example Plugins

<table>
<thead>
<tr>
<th>Resource</th>
<th>Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>scrypt [8], argon2d [4]</td>
</tr>
<tr>
<td>CPU</td>
<td>Hash functions</td>
</tr>
<tr>
<td>Chip rate limit</td>
<td>TPM</td>
</tr>
<tr>
<td>Cache</td>
<td>argon2d [4]</td>
</tr>
<tr>
<td>Network</td>
<td>Pythia [6]</td>
</tr>
</tbody>
</table>

Example Hash Functions

<table>
<thead>
<tr>
<th>Hash</th>
<th>Adopted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA2-512</td>
<td>US/NIST + EU/NESSIE</td>
</tr>
<tr>
<td>Whirlpool</td>
<td>Global/ISO + EU/NESSIE</td>
</tr>
<tr>
<td>SHA3-512</td>
<td>US/NIST</td>
</tr>
<tr>
<td>Steebo-512</td>
<td>Russia/FAPSI</td>
</tr>
<tr>
<td>Blake2-512</td>
<td>Open source projects</td>
</tr>
<tr>
<td>ChaCha20/Poly1305</td>
<td>Open source projects</td>
</tr>
<tr>
<td>AES/Poly1305</td>
<td>Open source projects</td>
</tr>
<tr>
<td>MD6</td>
<td>Open source projects</td>
</tr>
</tbody>
</table>

References

https://scrypt.com/download/scrypt-v1.9.1.tar.gz