
USENIX 2021

Cas Cremers
CISPA Helmholtz Center for Information Security

Britta Hale*
Naval Postgraduate School (NPS)

Konrad Kohbrok
Aalto University

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.
Two Group Messaging Paradigms

Groups are made of 1-to-1 connections (e.g. Signal)  
Group states are independent (e.g. MLS Draft 11, ART)
Two Group Messaging Paradigms

Groups are made of 1-to-1 connections (e.g. Signal)

Group states are independent (e.g. MLS Draft 11, ART)
Two Group Messaging Paradigms

Groups are made of 1-to-1 connections (e.g. Signal)

Group states are independent (e.g. MLS Draft 11, ART)
Post-Compromise Security (PCS)
Post-Compromise Security (PCS)

- A is compromised
Post-Compromise Security (PCS)

- A is compromised
- (Adversary is passive)
- A sends an update to B
Alice, the CEO, is returning from a business meeting.

On the way back, her phone is compromised and all data extracted.
Bob's Phone

Bob to Alice:
Have a good flight.
Bob’s Phone

Bob to Alice:
Have a good flight.

Groups using 1-1 keys

Groups using group keys
Bob’s Phone

Bob to Alice: Have a good flight.

Groups using 1-1 keys

Groups using group keys
Bob’s Phone

Bob to Alice: Have a good flight.

Alice to all: I’m back in the country, see you all on Monday!

Groups using 1-1 keys

Groups using group keys
Bob’s Phone

Bob to Alice:
Have a good flight.

Alice to all:
I’m back in the country, see you all on Monday!

Groups using 1-1 keys

Groups using group keys
Alice to all:
I'm back in the country, see you all on Monday!

Bob to Alice:
Have a good flight.

Groups using 1-1 keys

Groups using group keys
Bob's Phone

Bob to Alice:
Have a good flight.

Alice to all:
I'm back in the country, see you all on Monday!

Bob to Alice:
We closed the deal! Please keep this a secret until next month.

Groups using 1-1 keys

Groups using group keys
Bob to Alice:
Have a good flight.

Alice to all:
I’m back in the country, see you all on Monday!

Bob to Alice:
We closed the deal! Please keep this a secret until next month.
Design Space
Heal per group
Healing in one group prompts healing in others
Periodic healing in all groups
Global healing

Future groups healed

A

B

C

D

E

A

B

C

D

E

IDsig_pk

sig_pk1

sig_pk2

sig_pk3

sig_pk4
## Design Space

### Scheduling Updates for Confidentiality Keys

<table>
<thead>
<tr>
<th>Keys updated</th>
<th>Communication Activity Related</th>
<th>Periodic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Within group $i$</td>
<td>Within any group</td>
</tr>
<tr>
<td>Sym. group key: $g_{ki}$</td>
<td>Heal conf: group $i$</td>
<td>Heal conf: all groups</td>
</tr>
<tr>
<td></td>
<td>$2^{nd}$ Group Attack/NF</td>
<td>InfoLeak/NF</td>
</tr>
<tr>
<td></td>
<td>$O(1)$ Sym. Updates</td>
<td>$O(N)$ Sym. Updates</td>
</tr>
</tbody>
</table>

### Scheduling Updates for Authentication Keys

<table>
<thead>
<tr>
<th>Keys updated</th>
<th>Communication Activity Related</th>
<th>Periodic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Within group $i$</td>
<td>Within any group</td>
</tr>
<tr>
<td>Asym. group key pair: $(sk^i_A, pk^i_A)$</td>
<td>Heal auth: group $i$</td>
<td>Heal auth: all groups</td>
</tr>
<tr>
<td></td>
<td>$2^{nd}$ Group Attack/NF</td>
<td>InfoLeak/NF</td>
</tr>
<tr>
<td></td>
<td>$O(1)$ Asym. Updates</td>
<td>$O(N)$ Asym. Updates</td>
</tr>
<tr>
<td>Asym. global key pair: $(sk_A, pk_A)$</td>
<td>Heal auth: all groups + F</td>
<td>Heal auth: all groups + F</td>
</tr>
<tr>
<td></td>
<td>InfoLeak</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$O(1)$ Asym. Updates</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Post-Compromise Secure Signatures

- PCS is an accepted confidentiality security guarantee → can also be applied to \textit{authenticity}!
- Captures forgeries following a successful key update during an passive adversarial phase

Simple scheme: Rotating Signatures: New signature keys signed by old signature keys

\[ (\text{sig}_{pk1}, \text{sig}_{sk1}) \]

\[ \text{Compromise!} \rightarrow \text{Create an update} \rightarrow \text{Broadcast} \]

\[ (\text{sig}_{pk2}, \text{sig}_{sk2}) \leftarrow \text{gen()} \]
\[ s \leftarrow \text{sign} (\text{sig}_{sk1}, \text{sig}_{pk2} || \text{“update”}) \]

\[ \text{Adversary passive} \]

Check out the paper for more!

- Further attack scenarios and distinctions between the security of pairwise and group approaches
- Exploration of impacts of authentication and confidentiality, update distinctions and impacts
- PCS-SIG security experiment, realizable under further constructions
- How PCS-SIG security fits with existing messaging protocols
- Instantiation and proof of PCS-SIG

Contact:

Cas Cremers  
cremers@cispa.de

Britta Hale  
britta.hale@nps.edu

Konrad Kohbrok  
konrad.kohbrok@datashrine.de