PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4917 di Mercoledì 21 aprile 2021

Shadow attack: le alterazioni dei pdf firmati digitalmente

Oggi sono assai frequenti le situazioni nelle quali una offerta, in file PDF, viene inviata ad un cliente. Si chiede al cliente di firmare digitalmente il documento e restituirlo. Ma il processo è sicuro?

Penso che siano ben pochi i lettori di questi appunti che non abbiano avuto occasione di trovarsi nella situazione illustrata. I grandi vantaggi della firma digitale, posta sul documento PDF, sono evidenti: si risparmiano tempo e costi, rispetto allo scambio di documenti cartacei, ma, come spesso accade, non è tutto oro ciò che luccica.

Nel 2019, uno studio approfondito, sviluppato dai tecnici dell'Università della Ruhr, mise in evidenza come vi fossero numerose debolezze in molte applicazioni, che permettevano di visualizzare e firmare documenti PDF.

Lo schema adottato dai ricercatori era quello di avere a disposizione un documento PDF, che era stato firmato digitalmente da un soggetto terzo, e successivamente procedere alla manipolazione del documento, dopo che la firma era stata aggiunta al documento.

Sia quindi ben chiaro che l'attacco non riguardava tanto la firma, ma il contenuto del documento, che si riteneva non potesse essere più modificato, dopo essere stato firmato.

Il nome attribuito dai ricercatori a questo tipo di attacco è "shadow attack".

In questo scenario, ad esempio, i ricercatori hanno dimostrato come un'offerta, inviata da un'azienda a un cliente, e successivamente dal cliente firmata, poteva essere modificata nei prezzi. Il cliente riceveva pertanto una fattura di un importo più elevato e, a fronte delle sue rimostranze, gli veniva mostrata la copia dell'offerta, firmata digitalmente dal cliente, con gli importi alterati.

Se il cliente non aveva tenuto copia dell'offerta iniziale, la situazione poteva essere assai delicata.

Questo attacco si basa sul fatto che un documento PDF è composto da vari strati, alcuni dei quali possono essere modificati anche dopo che è stata apposta la firma digitale.

La modifica può essere a tre livelli:

- una modifica in base alla quale uno strato viene nascosto,
- una modifica in base alla quale uno strato con numeri e testo viene sostituito da un altro strato,
- una modifica in base alla quale viene utilizzato un secondo documento PDF, che sostituisce il precedente, trasferendo però la firma digitale.

I ricercatori hanno mostrato un esempio di questo attacco in cui, ad esempio, veniva sostituito l'IBAN indicato in una fattura, in modo che il bonifico giungesse ad altro destinatario.

Dopo che sono state messe in evidenza queste debolezze, i produttori di applicativi, che permettevano di visualizzare e firmare dei file PDF, hanno introdotto delle modifiche, che avrebbero dovuto porre rimedio a questa debolezza.

Raccomando vivamente a tutti i lettori di accertarsi che gli applicativi che utilizzano, per visualizzare e firmare file PDF, siano stati già debitamente aggiornati per fronteggiare questo attacco.

Adalberto Biasiotti

---

www.puntosicuro.it