Valutazione automatica dei rischi di sicurezza delle procedure di autenticazione bancarie

Roberto Carbone[1], Marco Pernpruner[1,2], Giada Sciarretta[1] e Silvio Ranise[1,3]
[1] Fondazione Bruno Kessler (FBK)
[2] Università degli Studi di Genova
[3] Università degli Studi di Trento

Negli ultimi anni abbiamo assistito ad una considerevole diffusione di servizi online, i cui innumerevoli vantaggi impattano in modo estremamente positivo sulla vita quotidiana: si pensi ad esempio alla comodità di poter compiere operazioni a distanza direttamente dalla propria abitazione. Questa tendenza ha recentemente subito una spinta a causa della situazione sanitaria globale, considerate anche le limitazioni sulla possibilità (e volontà) di spostarsi fisicamente per recarsi all'interno di filiali o negozi.

Tra le principali categorie di servizi online, troviamo sicuramente al primo posto per importanza quelli legati alla Pubblica Amministrazione, che permettono – anche grazie ad infrastrutture digitali nazionali come il *Sistema Pubblico di Identità Digitale* (SPID) [1] e la *Carta d'Identità Elettronica* (CIE 3.0) [2] – di effettuare operazioni che normalmente richiederebbero di recarsi fisicamente ad uno sportello comunale. Anche l'ambito bancario è stato protagonista di un notevole processo di digitalizzazione della sua offerta grazie a procedure di identificazione che forniscono elevati livelli di garanzia.

Se però da una parte il vantaggio legato allo sviluppo di queste nuove tecnologie è indiscutibile, dall'altra preoccupano i significativi rischi connessi con la sicurezza di tali piattaforme; in particolar modo, le procedure di autenticazione in contesto bancario sono attualmente oggetto di numerosi attacchi che hanno recentemente occupato le pagine di cronaca. Una delle principali strategie di attacco è indubbiamente il *phishing*, che permette ai malintenzionati di ottenere informazioni segrete (come password o PIN) ingannando gli utenti, convincendoli addirittura – in alcuni casi – ad effettuare operazioni a vantaggio degli attaccanti stessi. Uno studio Kaspersky sulle recenti minacce in ambito finanziario [3] riporta che nel corso del 2019 il *financial phishing* ha rappresentato il 51,4% della totalità degli attacchi perpetrati tramite phishing, con un aumento del 6,7% rispetto all'anno precedente. Oltre al phishing, un numero considerevole di attacchi vengono perpetrati tramite appositi *malware* sempre più potenti, che riescono a compromettere protocolli di autenticazione anche basati su più fattori: se al termine del 2019 il numero di pacchetti malevoli installati su dispositivi mobili era pari a 15410, nel primo quadrimestre del 2020 tale numero è quasi triplicato, arrivando a 42115 [3].

Per cercare di ridurre questo andamento, l'Unione Europea ha recentemente emanato la seconda versione della *Payment Services Directive* (PSD2) [4], una direttiva che – tra le altre cose – mira a fornire dei requisiti cui tutti i servizi bancari devono attenersi per migliorare la propria sicurezza intrinseca, in particolare riguardo all'autenticazione degli utenti.

Nel seguito, dettaglieremo i principali requisiti dettati dalla PSD2 sulle soluzioni di autenticazione riguardanti una vasta classe di servizi finanziari, analizzandone inoltre gli effetti su uno scenario reale tramite l'utilizzo di uno strumento automatico di valutazione dei rischi di sicurezza chiamato MuFASA (acronimo di *Multi-Factor Authentication Security Analysis*), sviluppato dalla Fondazione Bruno Kessler di Trento, nell'ambito di un dottorato congiunto con l'Università degli Studi di Genova.

PSD2: aspetti di sicurezza

Seppure l'obiettivo principale della PSD2 sia quello di favorire un sano aumento della competizione nel mercato dei pagamenti auspicando la nascita di servizi innovativi, particolare attenzione viene posta sugli aspetti di sicurezza sui quali tali servizi si devono basare. Per la gestione dell'identità digitale, considerata un elemento fondante per la sicurezza dei servizi, possiamo distinguere due requisiti fondamentali: la Strong Customer Authentication (SCA) e il Dynamic Linking.

I protocolli di autenticazione sono solitamente basati su un numero variabile di fattori di autenticazione, che possono rientrare in una delle seguenti categorie:

- *fattori di conoscenza*: elementi che l'utente deve conoscere, come ad esempio PIN o password;
- *fattori di possesso*: elementi che l'utente deve possedere, come ad esempio dispositivi per la generazione di OTP (*One-Time Password*) o *smartphone* su cui ricevere notifiche;
- *fattori di inerenza*: caratteristiche biometriche dell'utente, come ad esempio impronte digitali.

La *Strong Customer Authentication* prevede che l'autenticazione debba fare affidamento su più di una singola categoria di fattori di autenticazione (analogamente al concetto di *Multi-Factor Authentication*), unendo – ad esempio – fattori di conoscenza e di possesso, oppure di conoscenza e di inerenza per incrementare il livello di sicurezza dello specifico protocollo. Tuttavia, sono presenti alcune eccezioni che definiscono quando la SCA può non essere considerata obbligatoria (ad esempio per l'interrogazione del proprio saldo o per pagamenti inferiori a € 30). In questi casi, l'adozione o meno della stessa dipenderà dalla *Transaction Risk Analysis* (TRA), un'analisi automatica eseguita dal servizio di pagamento e finalizzata a valutare il rischio della transazione in corso (in base a fattori come l'istituto bancario, l'utente e la tipologia di operazione), il cui risultato determinerà la necessità o meno di effettuare la SCA.
Il *Dynamic Linking*, invece, richiede che il codice di autenticazione (normalmente un OTP) generato in seguito ad una SCA sia strettamente legato all'operazione in corso. Questo allo scopo di vanificare ogni tentativo di riutilizzare uno specifico codice di autenticazione da parte di un attaccante: anche qualora ciò avvenisse, infatti, l'attaccante potrebbe portare a termine solamente l'operazione avviata dall'utente stesso, senza quindi ottenere alcun beneficio reale. Inoltre, come ulteriore livello di sicurezza, all'utente devono sempre essere mostrati i dettagli dell'operazione in fase di autorizzazione, così da permettergli di valutarne la legittimità.

Conseguentemente, l'utilizzo di alcuni dispositivi comunemente usati fino a poco tempo fa non risulta più possibile. Considerando, ad esempio, dispositivi per la generazione di codici OTP basati sul tempo (come i token di sicurezza rilasciati da molte banche), il loro utilizzo non è più concesso a causa del *Dynamic Linking*, poiché (i) il codice generato non può essere in alcun modo legato all'operazione in corso (sarà solamente legato all'istante temporale nel quale è stato generato) e (ii) i dettagli dell'operazione non possono essere mostrati all'utente (il dispositivo non è provvisto di display per tale scopo, né è connesso alla rete per poter ricevere tali informazioni).

Valutazione automatica del rischio

Sulla base di quanto evidenziato finora, risulta fondamentale analizzare estensivamente la sicurezza di protocolli di autenticazione, specialmente in contesti sensibili come i servizi finanziari. Nel dettaglio, la nostra metodologia di valutazione del rischio è composta da due fasi: inizialmente, l'*analisi di sicurezza* permette di individuare quali tipologie di attaccanti riescono a compromettere con successo il protocollo analizzato, fornendo quindi una panoramica ad alto livello del suo grado di sicurezza; in seguito, l'*analisi del rischio* fornisce una prioritizzazione di tali attaccanti, rendendo così possibile una pianificazione delle mitigazioni da implementare con più urgenza.

Da un punto di vista pratico, l'*analisi di sicurezza* richiede una preventiva definizione delle capacità di ogni tipologia di attaccante considerata, al fine di poterne poi valutare l'effettiva efficacia sul protocollo. Per quanto riguarda l'*analisi del rischio*, si possono invece adottare alcune metodologie (ad esempio la *OWASP Risk Rating Methodology* [5]) che calcolano il rischio sulla base di due elementi: la *likelihood*, che indica la probabilità che un determinato evento abbia luogo; l'*impact*, che rappresenta l'eventuale impatto dell'evento qualora effettivamente si verifichi.
Sebbene la metodologia di analisi descritta possa essere messa in pratica anche manualmente, risulta estremamente importante automatizzarne l'esecuzione; questo porterebbe notevoli benefici legati alla riduzione sia delle tempistiche di svolgimento, sia della possibilità di errore umano.

MuFASA

Al fine di automatizzare la valutazione del rischio, il nostro approccio utilizza il software MuFASA (*Multi-Factor Authentication Security Analysis*) [6], sviluppato nel contesto delle attività di ricerca ed innovazione in cyber security della Fondazione Bruno Kessler.
MuFASA permette di effettuare l'analisi di protocolli di *Multi-Factor Authentication* al fine di stilare automaticamente una lista di attaccanti in grado – autonomamente o colludendo tra loro – di compromettere il protocollo specificato, insieme al relativo rischio.

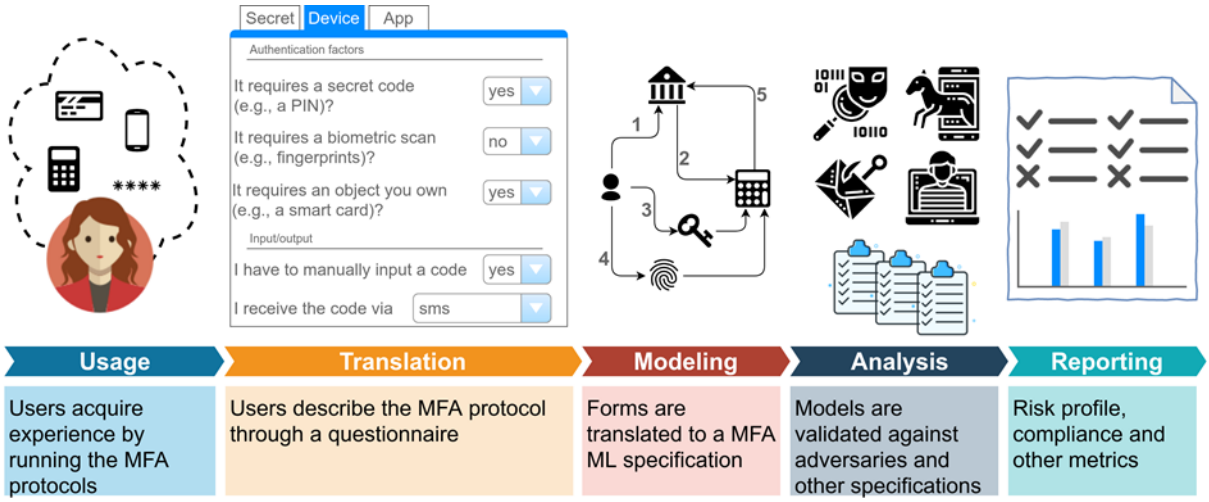

Figura 1. Fasi di MuFASA (fonte: [6])

Nel dettaglio, MuFASA si compone di cinque fasi (come illustrato in *Figura 1*):

1. *Usage*: l'utente entra a conoscenza di uno specifico protocollo e desidera verificarne la sicurezza;
2. *Translation*: l'utente descrive il protocollo desiderato rispondendo alle domande appositamente poste in linguaggio naturale all'interno di un questionario;
3. *Modeling*: grazie alle risposte fornite dall'utente, il protocollo viene tradotto dal linguaggio umano al linguaggio di specifica interno, che ne descrive le varie fasi dal punto di vista delle interazioni con l'utente;
4. *Analysis*: il protocollo fornito viene analizzato al fine di identificare gli attaccanti che hanno successo congiuntamente al relativo rischio;
5. *Reporting*: i risultati dell'analisi vengono stampati su un report PDF così da permetterne la facile fruibilità.

La possibilità di modellare il protocollo da analizzare tramite risposta ad un questionario riduce notevolmente la distanza tra MuFASA e i suoi utilizzatori, considerata la totale assenza di prerequisiti necessari per il suo utilizzo.

Esempio di analisi per un protocollo di online banking: pre e post PSD2

Consideriamo ora un esempio reale di protocollo di autenticazione utilizzato per l'approvazione dell'esecuzione di un'operazione bancaria (ad esempio un bonifico bancario) dal proprio computer; vedremo quindi l'evoluzione di tale protocollo per soddisfare la PSD2 e analizzeremo gli effetti di tale normativa sulla sicurezza complessiva.

Figura 2. Il protocollo analizzato prima dell'avvento della PSD2

Prima della PSD2, come illustrato in *Figura 2*, l'utente dapprima inseriva le proprie credenziali per autenticarsi sulla propria piattaforma di *online banking*, disponeva l'operazione desiderata e successivamente generava un OTP tramite uno token di sicurezza in suo possesso, inserendo infine tale codice all'interno della schermata di autorizzazione del proprio *online banking*.
I risultati di MuFASA su questo protocollo identificano quattro attaccanti[3] in grado di violare la sicurezza del protocollo; tali attaccanti sono descritti in *Tabella 1*:

[3] Per maggiore chiarezza, in questo documento consideriamo solamente attaccanti che singolarmente riescono a compromettere il protocollo. Non consideriamo invece attaccanti che colludono tra loro per aumentare le loro capacità.

Attaccante	Descrizione	Rischio
Eavesdropping Software	Applicazioni malevole che intercettano le informazioni inserite dall'utente (ad esempio, un *keylogger*)	**ALTO**
Man in the Browser	Applicazioni o estensioni malevole che hanno il controllo del browser dell'utente e riescono ad acquisire le informazioni immesse dall'utente, oltre ad essere in grado di alterare le schermate mostrate	**ALTO**
Shoulder Surfer	Persone fisiche che – situate in prossimità dell'utente – riescono a visualizzarlo mentre compie l'operazione, compromettendo le informazioni segrete	**MEDIO**
Social Engineer	Attaccanti in grado di ingannare l'utente, portandolo a rivelare informazioni o compiere operazioni a loro vantaggio (ad esempio, tramite *phishing*)	**MEDIO**

Tabella 1. Attaccanti singoli efficaci prima dell'avvento della PSD2

A scopo esemplificativo, lo *Shoulder Surfer* può compromettere il protocollo essendo in grado di vedere l'inserimento delle credenziali e l'OTP mostrato sul display del token fisico; in particolare, tramite le credenziali può accedere all'account dell'utente e disporre qualunque operazione desideri, riutilizzando poi l'OTP nell'intervallo di tempo di validità per autorizzare l'operazione.

Figura 3. Il protocollo analizzato dopo l'avvento della PSD2

In seguito all'avvento della PSD2, come illustrato in *Figura 3*, l'utente dapprima inserisce le proprie credenziali per autenticarsi sulla propria piattaforma di *online banking*, quindi – dopo aver disposto operazione desiderata – riceve sul proprio *smartphone* una notifica *push*. Infine, cliccando sulla notifica *push*, visualizza i dettagli dell'operazione in corso, oltre ad un codice OTP da riportare manualmente all'interno della schermata di autorizzazione del proprio *online banking*.
Analizzando questo protocollo, MuFASA non ha riscontrato alcun attaccante singolo in grado di compromettere il protocollo. Infatti, l'utente è ora consapevole dell'operazione in corso, i cui dettagli gli vengono mostrati in seguito a click sulla notifica *push*; inoltre, il codice di autenticazione è legato alle specifica operazione, pertanto – come accennato in precedenza – un eventuale attaccante che ne venisse in possesso non potrebbe effettuare alcuna operazione differente da quella voluta dall'utente, all'interno di alcuna sessione che non sia quella in uso dall'utente. Considerando ad esempio lo *Shoulder Surfer*

analizzato in precedenza, questo non risulta più in grado di compromettere il protocollo non potendo più disporre un'operazione a suo piacimento.

In questo caso, risulta quindi evidente il notevole incremento di sicurezza indotto dall'adozione della PSD2. Per comprendere lo stato di sicurezza delle procedure di autenticazione bancarie prima e dopo la PSD2 si potrebbe utilizzare MuFASA per ogni singola soluzione, analizzandone successivamente i risultati.

Conclusioni

Per poter garantire la sicurezza dei servizi online, in particolare in contesti sensibili come quello finanziario, la sicurezza delle procedure di autenticazione – che vengono utilizzate anche per autorizzare alcune transazioni – deve essere tenuta altamente in considerazione. A tal fine, risulta di notevole importanza la possibilità di effettuare in maniera automatica analisi precise ed accurate dei protocolli di autenticazione al fine di esplorare le possibili alternative e scegliere quella più adatta allo scenario di utilizzo.

Il tool MuFASA, sviluppato all'interno della Fondazione Bruno Kessler, soddisfa tali scopi permettendo l'analisi di sicurezza e del rischio di protocolli di *Multi-Factor Authentication*. La semplice modalità di specifica del protocollo da analizzare, che avviene tramite un questionario ad alto livello, limita le barriere da parte dell'utente, che non dovrà più necessariamente conoscere specifici linguaggi per la modellazione dei protocolli.

MuFASA può essere utilizzato in diversi scenari: da una parte per l'analisi e il confronto delle soluzioni esistenti sul mercato, in termini di sicurezza, rischio, usabilità e conformità ai requisiti imposti dalla PSD2; dall'altra in fase di progettazione di nuovi protocolli di autenticazione, effettuando quindi una *what-if* analisi per valutare il miglior compromesso tra usabilità e sicurezza.

Riferimenti

[1] Agenzia per l'Italia Digitale. "*SPID – Sistema Pubblico per l'Identità Digitale*". https://www.spid.gov.it/

[2] Ministero dell'Interno. "*Carta d'identità elettronica*". https://www.cartaidentita.interno.gov.it/

[3] Kaspersky. "*Financial Cyberthreats in 2019*". https://securelist.com/financial-cyberthreats-in-2019/96692/

[4] The European Parliament and the Council of the European Union. "*Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC*". In: Official Journal of the European Union. http://data.europa.eu/eli/dir/2015/2366/oj

[5] The Open Web Application Security Project. *"OWASP Risk Rating Methodology*". https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

[6] Sinigaglia Federico, Carbone Roberto, Costa Gabriele, Ranise Silvio. "*MuFASA: A Tool for High-level Specification and Analysis of Multi-factor Authentication Protocols*". In: Emerging Technologies for Authorization and Authentication. ETAA 2019. Lecture Notes in Computer Science, vol 11967. Springer, Cham. https://doi.org/10.1007/978-3-030-39749-4_9