Hacking dei sistemi di raccolta del *voto* e del *consenso* online

Prof. Giovanni Ziccardi
Università degli Studi di Milano
http://www.ziccardi.org

Perugia, 25 aprile 2013
@Festival Internazionale del Giornalismo

Tre fonti/studi *open*

- *David Jefferson*, *Aviel D. Rubin*, *Barbara Simons* e *David Wagner*, **Analyzing Internet Voting Security, Communications of the ACM**, Ottobre 2004, Vol. 47, n. 10, p. 59 e ss.
- *Scott Wolchok*, *Eric Wustrow*, *Dawn Isabel* e *J. Alex Halderman*, **Attacking the Washington, D.C. Internet Voting System**, in Proc. 16° Conference of Financial Cryptography & Data Security, Febbraio 2012.
- *David Talbot*, **Why can't you vote online**, MIT Technology Review, 5 Novembre 2012.

(1)

IL PASSATO E I “SEMI”

Dieci anni fa...

Un primo **studio** interessante. Analisi della **sicurezza** del voto via Internet e una sorta di proposta di **assesment** a firma D. Jefferson, A. D. Rubin, B. Simons e D. Wagner.

Si analizza il sistema **SERVE** (Secure Electronic Registration and Voting Experiment).

Sistema sviluppato da **Accenture** con altri partner e pensato per il **Dipartimento della Difesa** USA e per il suo *Federal Voting Assistance Program*, programma per agevolare nel voto tutti i cittadini USA residenti **all'estero**, soprattutto militari, corpi diplomatici e loro famiglie.

Il fine di SERVE

Sia **registrarsi** per votare, sia **votare** via Internet da qualsiasi parte del mondo.

Si propone anche di essere una completa e indipendente **Testing Authority** che sia qualificata e "certificata" dallo Stato e che raccolga voti **reali**.

Chi vota deve superare **tre fasi**: 1) **iscriversi** a SERVE; 2) **registrarsi** per il voto; 3) votare in una o due **brevi sessioni** di voto da un PC connesso a Internet (sistema MS Windows ed Explorer o Netscape, javascript, java e activeX e session cookies) senza hardware o software aggiuntivo.

Come funziona in pratica

Quando una persona si **registra** online per votare, le informazioni che lo riguardano sono memorizzate sul **server centrale** per essere recuperate **successivamente** dal **Local Election Official** (che custodisce un database aggiornato dei votanti).

Quando una persona **vota**, il voto completo di tutti i dati è memorizzato sul server centrale e viene poi **scaricato** dal LEO che lo custodisce per lo spoglio/conteggio/verifiche.

Comunicazione tra utente e web server centrale: avviene via SSL. Stabilita la connessione, viene "downloadato" un *control* Active-x che permette al browser di eseguire **funzioni non solite**.

Prima prova nel 2004

Prima prova su base volontaria del sistema: gestione di **100.000** voti nel giro di un anno, sia primarie sia elezioni generali.

Nelle elezioni generali "tradizionali" del 2000 erano stati "spogliati" oltre 100 milioni di voti "fisici".

Il target sono **6 milioni di votanti** UOCAVA (sigla che indica i cittadini US "bloccati" all'estero).

È un progetto **enorme** e multimilionario per il voto reale con strumenti digitali.

I problemi...

I DRE (direct recording electronic) voting systems sono stati **criticati** per vari problemi di sicurezza: 1) software **proprietario** e **chiuso**; 2) non viene controllato con cura il software durante il processo di certificazione e di qualità dello stesso; 3) sono particolarmente vulnerabili ad attacchi portati da **insider**; 4) manca una **verifica** manuale o **cartacea** di confronto che possa ovviare ai problemi precedenti.

SERVE, in più, è basato su PC e Internet e quindi aggiunge a quelli sopra i problemi di sicurezza **tipici** (DOS, spoofing, attacchi con virus) di quegli "ambienti".

Natura e esito di attacchi

Sono attacchi su **larga scala**.

Possono essere lanciati da ogni **parte** del mondo e con qualsiasi motivazione (dal singolo che protesta, sino a una società/ organizzazione con fondi illimitati).

Possono portare a **sfiducia** o disaffezione nel sistema, alla violazione della **privacy**, a **compravendita** di voti, a **switching** dei voti per alterare l'esito delle elezioni.

Possono essere completamente **nascosti** e possono avere un effetto devastante sulla **fiducia** pubblica nel momento in cui sono scoperti.

Che tipo di attacco?

Può essere **semplice**, e portato anche da una sola persona con medie capacità.

Non c'è bisogno che sia **organizzato** da una fazione politica, o da uno Stato estero, o da gruppi di terroristi.

Vedremo che basta un **gruppetto** di 3 o 4 studiosi per far saltare il sistema di un intero Stato e da centinaia di migliaia di voti.

#1 (un)auditing

Il primo problema critico di molti sistemi "senza carta" è la mancanza di possibilità di un **auditing** sull'intero processo di voto che permetta al **votante** di verificare che il voto registrato dalla macchina sia lo **stesso** voto che ha immesso e che vede mostrato sullo schermo.

Se occorrono problemi **successivi** al voto durante lo spoglio, non c'è alcun processo indipendente di auditing precedente che possa **aiutare** a risolvere i problemi.

La possibilità di **verifica** del voto è l'unico rimedio contro attacchi dall'interno o malfunzionamenti.

#2 Privacy

La privacy si protegge di solito con sistemi **crittografici**.

Trasmissione cifrata “in transito”, e poi a **decifrare** è solo l’ufficio che effettua lo spoglio.

Una volta ricevuto, il voto, lo stesso viene **separato** dall’identità del votante e viene cifrato di **nuovo**.

Problema di sicurezza che deriva da una eventuale **curiosità** di un ufficio elettorale locale e dalla possibilità per lo stesso di vedere come i **singoli** votino.

#3 Compravendita di voti

Su larga scala la compravendita viene **facilitata** dall'elettronica.

Si vendono i dati **identificativi** e la **password** del votante o la **chiave privata** crittografica.

Una soluzione blanda può essere impedire di immettere il voto dallo stesso *indirizzo* IP, ma **non** è sempre efficace.

#4 Attacchi su larga scala

Numericamente, che **impatto** può avere un attacco elettronico?

Su quanti voti può influire rispetto, ad esempio, a **brogli** tradizionali?

Può un **singolo**, in un ambiente **non elettronico**, alterare decine di migliaia di voti?

In ambiente elettronico, sì.

#5 Controllo del PC

In sistemi di voto online, **"l'autorità"** non ha il **controllo** del dispositivo usato, ossia il PC del votante, e della sua sicurezza.

Terze parti possono **controllare** il PC, e nel nostro caso il PC dell'utente diventa immediatamente un sistema **critico**, e anche i software pre-installati possono porre rischi.

Si pensi ad attacchi di **spoofing** o Man-in-the-Middle, per attaccare la privacy del votante (creazione di SSL gateway per bypassare anche il sistema SSL) o semplicemente l'utilizzo di keyloggers o trojan.

(2)

IL PRESENTE REALE

“2012 ATTACCO A WASHINGTON D.C.”

Attacco a Washington D.C.

Siamo nel febbraio **2012**, e appare uno studio di Wolchok, Wustrow, Isabel e Halderman.

Nel 2012, l'amministrazione di Washington D.C. sviluppa un progetto **pilota** di voto via Internet per soggetti residenti al di fuori dello Stato.

Prima di sviluppare il sistema, il *District* organizza una sorta di "**gara**": una **finta elezione** dove chiunque è portato a testare/violare il sistema, o a cercare di provare la sua insicurezza.

A **48 ore** dalla messa **live** del sistema, gli autori dello studio lo **violano** e ottengono il **controllo completo** dell'intero sistema di elezioni.

Cosa fanno gli attaccanti

Cambiano ogni singolo voto (*falsificazione*).

Rivelano ogni voto **segreto** abbinando **votante** a **voto** (*attacco alla privacy*).

Gli "ufficiali" deputati alla sicurezza del sistema elettorale non rilevano **alcuna** intrusione fino a quando non viene suggerita dagli hacker, e almeno dopo **due** giorni lavorativi dal fatto.

Primo caso di analisi muovendo dalla prospettiva di un **attaccante** in un ambiente reale.

I rischi preliminari evidenziati

Sistema basato su **web**.

Sistema che **deve** mantenere **l'integrità** del risultato elettorale.

La **segretezza** delle scelte operate dai votanti è **essenziale**.

Deve essere un sistema sempre **disponibile** e non compromesso ma su un network **aperto** (cosa non facile...).

Deve servire votanti che si collegano da dispositivi **non sicuri**.

Sistema open source

Test di attacco che dura **4 giorni**.

Prospettiva di attacco: ricerca delle **vulnerabilità** su fonti pubbliche, ricerca di vulnerabilità che permettessero di ottenere il **controllo** del sistema, **rivelare** il voto segreto e **alterare** i risultati della finta elezione.

L'attacco ha **successo**, e il District **abbandona** il progetto di sviluppare un simile sistema.

Metodo corretto di testing: permettere un attacco **reale** su una elezione **finta**.

DVBM

Sistema di **Digital Vote By Mail.**

Architettura **open source** sviluppata con una fondazione. Ruby on Rails framework, Apache web server e mySQL come database relazionale.

Le informazioni **generali** sul voto (nomi dei votanti, indirizzi, credenziali "sotto hash" e esito del voto) sono nel database mySQL.

I voti sono **cifrati** e memorizzati nel filesystem.

Le sessioni e gli user id sono in un **cookie** di sessione cifrato nel browser dell'utente.

L'infrastruttura

Ci sono **firewall**, connessioni **https** e computer basati su GNU/Linux.

Come funziona: serve per militari e "overseas residents".

Alcuni **mesi** prima della elezione, ogni possibile elettore riceve una **lettera** con la "posta fisica" che contiene le **credenziali** per il sistema (ID number del votante, nome registrato, codice di residenza e un **PIN** di **sedici** caratteri che lo identifica).

Come vota?

Il votante sceglie se votare per **posta** o in **digitale**.

Si **logga** con le credenziali, e **conferma** la sua identità.

Gli viene fornita una **scheda bianca** in PDF.

Se usa la posta, la **stampa** e la **spedisce** dopo aver votato.

Se usa il **digitale**, la **marca/segna** con un PDF reader e la salva sul suo **computer,** poi la **uploada** al sistema di voto centrale che mostra un messaggio "**grazie per aver votato**" se il processo va a buon fine.

Il votante non si può collegare **una seconda volta:** viene portato sempre alla pagina "grazie".

Come attaccano gli hacker

Attaccano come prima cosa la **applicazione** sul server "elettorale".

In primis analizzano il **codice**.

Si interessano ad alcuni passaggi vulnerabili, e in particolare **i)** alla fase del **login**, **ii)** alla fase **dell'upload** della scheda, e **iii)** alla **comunicazione** con il database elettorale.

Il fatto che il codice fosse open source ha **accelerato** la conoscenza dei punti deboli, ma anche in un codice chiuso, scrivono gli hacker. si sarebbero potute sfruttare le **stesse** vulnerabilità (anche se con altri metodi).

Shell-injection vulnerability

Dopo qualche ora, scoperta la prima vulnerabilità.

Permette di compromettere la applicazione elettorale su server.

La vulnerabilità viene trovata nel codice di cifratura della scheda di voto uploadata dal votante, in una locazione **temporanea** su disco.

Attacchi successivi

Furto di dati **segreti**. Hanno recuperato la chiave **pubblica** utilizzata per cifrare le schede. Nonostante il nome "pubblico", va tenuta comunque segreta perché può permettere l'accesso al sistema di storage dei voti.

Accesso al database.

Cambiamento di voti presenti e futuri. Hanno **sostituito** i voti reali con voti di loro preferenza.

Rivelazione di voti **passati** e **futuri** e attacco alla segretezza del voto: hanno trovato i voti **prima** che fossero cifrati in una directory temporanea.

Ulteriori attacchi

Scoperta delle **vere credenziali dei votanti**.

Scoprono un *file* in formato PDF lungo 937 pagine in una directory temporanea che conteneva tutte le **lettere** di istruzione inviate con le credenziali.

Se questo file fosse stato reso pubblico il giorno prima del voto, sarebbe stato impossibile **rispedire** le lettere in tempo e questo attacco avrebbe fatto **saltare** le elezioni.

Cancellazione delle tracce alterando i log.

Modificano la pagina "grazie" con la canzone di battaglia della loro Università, per lasciare una traccia poco invasiva dell'attacco.

Attacco (anche) al network

Non solo le applicazioni sul server, ma il **network** stesso necessario a gestirle è vulnerabile ad attacchi.

Infiltrazione nel terminale del server (password di root, etc)

Router e switch con relative vulnerabilità.

Webcam sul network che puntavano alle sale server e che permettevano di vedere che tipo di server erano utilizzati.

Conclusioni

Attacco cui viene data risposta dopo 36 ore, a sistema scollegato.

L'attacco non era visibile dai log attuali.

Trovare le tracce ha richiesto diversi giorni di analisi e lo "spulciare" nei backup.

(3)

PERCHE' NON VOTARE ONLINE

MIT

Conclusioni: MIT 2012

"Perché non potete votare online", *David Talbot*.

a) I problemi fondamentali di sicurezza ancora **non sono** risolti.

b) Si entra in un mondo complesso quando invece la sicurezza è data dalla **semplicità**.

c) Un sistema da 22 milioni di dollari come quello di Accenture è stato dismesso dopo i **test** degli hacker. Si pensi alle risorse necessarie per attivare un sistema valido su rete aperta.

GRAZIE!

Prof. Giovanni Ziccardi

@gziccardi

giovanni.ziccardi@unimi.it

http://www.ziccardi.org