UNIVERSITÀ DEGLI STUDI DI BOLOGNA

DIPARTIMENTO DI ELETTRONICA INFORMATICA E SISTEMISTICA

Verifica della conformità del sistema u-Vote alle norme europee sui sistemi di voto elettronico

Relazione di sintesi

Roberto Laschi
Università di Bologna
Viale del Risorgimento, 2
40136 Bologna (BO)
roberto.laschi@unibo.it

Marco Prandini
Università di Bologna
Viale del Risorgimento, 2
40136 Bologna (BO)
marco.prandini@unibo.it

Marco Ramilli
Università di Bologna
Via Venezia, 52
47023 Cesena (FC)
marco.ramilli@unibo.it

Revisione 6 - 13 gennaio 2010

Executive summary

Per rispondere alle esigenze di elezione delle Commissioni di Valutazione per il reclutamento dei professori e dei ricercatori, il Ministero dell'Istruzione, dell'Università e della Ricerca ha richiesto nel 1998 al CINECA la realizzazione di un sistema di voto telematico.

u-Vote è l'ultima generazione di tale sistema, risultato del processo di innovazione tecnologica intrapreso dal CINECA al fine di mantenere le caratteristiche di sicurezza, affidabilità e robustezza del sistema di voto telematico del 1998, introducendo al contempo nuove funzionalità utili ad un corretto e razionale svolgimento del processo elettorale.

Il CINECA ha commissionato al Dipartimento di Elettronica Informatica e Sistemistica (DEIS) dell'Università di Bologna l'esecuzione di un insieme significativo di test di laboratorio atti a verificare la funzionalità e la sicurezza del sistema u-Vote nelle condizioni più realistiche di funzionamento, ivi incluse situazioni di guasto, errore, ed interferenza volontaria da parte di terzi.

Questa relazione riassume le attività svolte dal gruppo di lavoro del DEIS per accertare la conformità di u-Vote alle norme internazionali che riguardano l'intera categoria di sistemi di cui esso fa parte, illustrando:

- gli elementi essenziali di analisi delle raccomandazioni internazionali in materia di definizione delle tipologie di verifiche da condurre;
- le scelte metodologiche ed operative che hanno condotto alla progettazione, realizzazione e documentazione dei test eseguiti.

Questo documento riporta in forma sintetica la struttura dei test eseguiti, i risultati osservati, e le raccomandazioni del gruppo di lavoro per un corretto utilizzo del sistema; i dettagli delle singole procedure di test ed i risultati puntuali della loro esecuzione sono invece riportati in allegati separati (rispettivamente: u-Vote Test Plan ed u-Vote Test Report).

Gli aspetti di maggior rilevanza emersi dall'attività descritta possono essere, in estrema sintesi, così esposti:

- il sistema è reputato adatto all'uso per il quale è stato progettato;
- non risultano presenti vulnerabilità sfruttabili, se sono rispettate le ipotesi di corretto impiego del sistema richieste dal CINECA, e cioè essenzialmente che la sicurezza fisica e l'integrità del sistema operativo delle postazioni di voto siano garantite tramite la predisposizione di seggi secondo le migliori pratiche riportate nel Test Report finale, che individuano dettagliatamente le condizioni ambientali e di configurazione da rispettare per garantire il massimo livello di sicurezza.

Indice

Abstract

Questa relazione riassume le attività svolte dal gruppo di lavoro del Dipartimento di Elettronica Informatica e Sistemistica (DEIS) dell'Università di Bologna, delegato dal CINECA (Consorzio Interuniversitario per il Calcolo Automatico dell'Italia Nord Orientale) all'attività di verifica della conformità del proprio sistema di voto elettronico (u-Vote) alle norme internazionali che riguardano tale categoria di sistemi.

Lo scopo di questo documento è quello di illustrare le scelte metodologiche ed operative che hanno condotto alla progettazione, realizzazione e documentazione dei test eseguiti. Poiché non esiste un vero e proprio quadro normativo di riferimento, si ritiene infatti indispensabile motivare ogni passo logico che ha portato dall'analisi delle raccomandazioni internazionali in materia alla definizione delle tipologie di verifiche da condurre, alla definizione di piani di test dettagliati, ed infine alla loro esecuzione e relativa documentazione dei risultati.

Per mantenere la necessaria leggibilità, questo documento riporta solo in forma sintetica la struttura dei test eseguiti, i risultati osservati, e le raccomandazioni del gruppo di lavoro per un corretto utilizzo del sistema nei casi in cui condizioni al contorno differenti da quelle dell'ambiente di testing possano influire significativamente sul comportamento del sistema medesimo.

I dettagli delle singole procedure di test ed i risultati puntuali della loro esecuzione sono invece riportati in allegati separati (rispettivamente: *u-Vote Test Plan* ed *u-Vote Test Report*), utilizzabili dagli enti interessati all'utilizzo del sistema al fine di determinarne la consistenza ai propri requisiti (ed eventualmente al fine di ripetere autonomamente i test).

Contesto

Per rispondere ad una precisa esigenza del Ministero dell'Università e della Ricerca, nel 1998 il CINECA ha realizzato un sistema di voto telematico che fino ad oggi è stato utilizzato come sistema di voto ufficiale per la composizione delle Commissioni di Valutazione e per l'elezione degli Organi Accademici di alcune Università italiane.

Per risolvere il problema di naturale obsolescenza delle macchine e dell'apparato tecnologico del sistema di voto telematico, il CINECA ha avviato un processo di innovazione tecnologica che ha portato al nuovo sistema di voto elettronico u-Vote. u-Vote mantiene le caratteristiche di sicurezza, affidabilità e robustezza del sistema di voto telematico del 1998, introducendo al contempo nuove funzionalità utili ad un corretto e razionale svolgimento del processo elettorale.

Il CINECA ha commissionato al DEIS l'esecuzione di un insieme significativo di test di laboratorio atti a verificare la funzionalità e la sicurezza del sistema u-Vote nelle condizioni più realistiche di funzionamento, ivi incluse situazioni di guasto, errore, ed interferenza volontaria da parte di terzi. Il DEIS ha formato allo scopo un gruppo di lavoro d'ora in avanti chiamato DEIS Working Group (*DWG*).

Metodologia

Definizione della normativa di riferimento

Non esiste in Italia, né a livello di Unione Europea, una precisa norma tecnica che stabilisca gli standard a cui attenersi nella progettazione e realizzazione di un sistema per il voto elettronico. La prima parte dell'attività del DWG quindi è stata la ricognizione della documentazione esistente che potesse essere utilizzata allo scopo di definire una linea normativa accettabile. I risultati di questa attività sono sintetizzati di seguito, e dove meritevoli di approfondimento ripresi nel dettaglio nell'allegato *La regolamentazione delle procedure di voto condotte con sistemi elettronici ed informatici: un confronto tra gli approcci statunitense ed europeo.*

Senza dubbio il documento di riferimento risulta essere la *Recommendation Rec(2004)11* adottata dal Comitato dei Ministri del CoE il 30 settembre 2004 ed intitolata "Legal, operational and technical standards for e-voting" [1]. Anche una lettura superficiale di tale testo, però, evidenzia un problema di implementabilità. Nelle *Recommendation* sono esposti di tutti i principi che devono regolare in termini generali l'adozione di macchine come ausilio alle procedure di voto, ma non in modo "testabile": non vi è alcuna indicazione sufficientemente specifica da poter essere mappata in una procedura di verifica che permetta di attestare la conformità di un sistema candidato a tali principi.

Da questo punto di vista la ricognizione ha invece individuato negli Stati Uniti un esempio di pragmatismo che ha prodotto strumenti avanzati ed efficaci per normare, testare e quindi certificare sistemi di ausilio al voto. La *Election Assistance Commission* si è occupata di redigere tutti i documenti di principio (sebbene questo termine sia da considerare declinato in modo molto meno astratto e generale che non nella *Recommendation*), tra cui spiccano per i nostri fini le *Voluntary Voting System Guidelines* o (*VVSG*) [2]. Il *National Institute for Standards and Technology* coordina la definizione delle precise procedure di testing della conformità dei sistemi alle *VVSG*.

Dal punto di vista operativo, quindi, si è voluto trarre vantaggio dall'importante lavoro svolto dagli organismi USA per realizzare la struttura dei test, naturalmente però finalizzando questi alla verifica della conformità alla *Recommendation* europea. Come meglio spiegato nel citato allegato, l'operazione di mappatura tra principi della *Recommendation* europea e procedure collegate alle *VVSG* è risultata non semplicissima. I problemi fondamentali sono risultati essenzialmente: da un lato, la presenza nella *Recommendation* di norme che esprimono requisiti per la conduzione dell'elezione che poco hanno a che fare con l'utilizzo di sistemi elettronici, e quindi non trovano espressioni omologhe nelle *VVSG;* dall'altro la succitata mancanza di generalità delle *VVSG* che, in alcuni punti, sono dettate più dalla consapevolezza di dover trattare sistemi specifici (perché già largamente diffusi) che dalla più corretta volontà di esprimere principi di ampia validità.

In definitiva però non si sono riscontrate nemmeno difformità concettuali tali da precludere l'adattamento delle *VVSG,* e delle metodologie di testing da esse derivate, in funzione della definizione di un *Test Plan*.

Un intervento più incisivo sulla lettura della *Recommendation* invece è stato fatto alla luce di analisi critiche reperibili in letteratura [3], che evidenziano oggettivi problemi di coerenza interna del documento. Poiché tali analisi, anche in questo caso, non contraddicono sostanzialmente la *Recommendation* ma ne riorganizzano in modo più razionale i contenuti, si è ritenuto opportuno accoglierne il contributo.

Passaggio dalla norma di riferimento al piano di test per il sistema u-Vote

Un sistema come quelli elettronici per il voto oggetto della presente attività è un insieme complesso ed articolato di componenti hardware e software, ognuno dei quali può essere scelto in modo diverso in ogni specifica istanza del sistema medesimo, per realizzare il risultato più soddisfacente in termini di affidabilità, costi, rispondenza alla tipologia di consultazione elettorale, reperibilità sul mercato, ecc..

Il lavoro dell'ente deputato a certificare la conformità di un particolare sistema alla normativa deve essere reso il più possibile indipendente da tali scelte. Si ha quindi la necessità di definire una procedura di derivazione del *Test Plan*, piuttosto che il *Test Plan* stesso, in modo da poterla applicare nel modo più efficiente ed ottenere di volta in volta *Test Plan* rispondenti alle peculiarità che i sistemi da certificare presentano, in funzione del fornitore e del tempo di progettazione e realizzazione.

Sebbene in questo caso specifico il DWG abbia ricevuto dal CINECA l'incarico ultimo di testare un'istanza ben precisa del sistema u-Vote, di comune accordo si è deciso di seguire la strada più generale ed organica, stimando che l'investimento di tempo e risorse necessario possa essere ripagato sul medio e lungo periodo dall'adattabilità delle procedure prodotte alle versioni di u-Vote che certamente seguiranno quella oggetto degli attuali test. I passaggi svolti sono stati quindi:

(a) Mappatura delle *Recommendation* sulle *VVSG* – Come descritto al punto precedente di questa sezione, si è tracciato il parallelo tra le raccomandazioni europee e le norme USA per poter poi utilizzare nei passi successivi quanto già esistente in materia di certificazione per queste ultime; è stata necessaria una riorganizzazione delle raccomandazioni europee, che spesso fanno riferimento in luoghi distinti a proprietà più sensatamente testabili in modo unitario.

(b) Realizzazione dell'*Abstract Test Plan* (*ATP*)– Si è effettuata una riscrittura delle norme dettagliate al passo precedente in forma di istruzioni per il laboratorio di test, senza tuttavia includere alcun dettaglio relativo al sistema da testare: in altre parole, viene esplicitato in termini concettuali cosa si deve testare per verificare la conformità al dettato di ogni articolo normativo, cercando di esplicitare anche, nel massimo grado consentito dal vincolo di non perdere di generalità, in che modo effettuare i test e che risultati considerare rilevanti. Le voci che compongono l'*ATP* sono detti *Derived Test Requirement* (*DTR*), cioè i requisiti di test derivati [dalle corrispondenti norme].

(c) Realizzazione del *Test Plan* – Dato il *Technical Documentation Package* del sistema, i *DTR* possono essere trasformati in istruzioni dettagliate su come eseguire i test sul sistema, introducendo le necessarie specifiche relative alla particolare configurazione hardware, software, e di contesto d'uso previsto.

Vale la pena notare che i risultati intermedi descritti ai punti (a) e (b) possono, se considerati qualitativamente e quantitativamente soddisfacenti, essere fatti propri dagli organismi deputati a livello più alto alla certificazione dei sistemi di voto per stabilire le linee guida generali del processo di validazione dei sistemi, non essendo in alcun modo legati al caso specifico qui trattato.

DTR e ATP

Struttura dei DTR

I requisiti di testing derivati dalle norme specificano che tipo di funzionalità o proprietà del sistema debba essere verificata per poter giudicare la conformità del sistema stesso alla corrispondente norma.

I principi tenuti in considerazione nella scrittura dei *DTR* sono essenzialmente:

1. Ove possibile, specificare il test sotto forma di coppia (stimolo da applicare al sistema, risposta attesa); indicare se appropriato i valori nominali, le fasce di valori accettabili e non per gli stimoli e le risposte;
2. Nei casi in cui non sia adottabile il modello stimolo-risposta per motivi di costo o strutturali, indicare la necessità che il laboratorio di testing possa esaminare il progetto hardware e/o il codice sorgente per verificare non solo la rispondenza logica del sistema al comportamento atteso, ma anche l'adozione di tecniche ingegneristiche allo stato dell'arte (principalmente in termini di affidabilità e robustezza).

Sintatticamente, i *DTR* devono riportare:

1. Il requisito a cui fanno riferimento, cioè la voce normativa il cui rispetto deve essere determinato dal test illustrato; si deve prevedere il caso che un *DTR* possa svolgere il ruolo di verificare in tutto o in parte la rispondenza a più norme, indicando con chiarezza i riferimenti incrociati;
2. L'elenco delle asserzioni da testare per verificare il requisito; spesso queste si ricondurranno direttamente al testo della corrispondente norma, o ne saranno una rielaborazione più facilmente implementabile; possono essere sia positive (verifica di una determinata risposta allo stimolo) che negative (verifica che uno stimolo non produca una determinata risposta);
3. Per ogni asserzione, se necessario, quali richieste il laboratorio deve fare al produttore del sistema per essere poi in grado di trasformare il *DTR* in una voce concreta del *Test Plan*;
4. Ad ogni asserzione sono associate una o più procedure di test, esplicitamente se queste sono specifiche dell'asserzione considerate, o implicitamente se il *DTR* rimanda alle procedure di test di altri *DTR*.

Organizzazione generale dei DTR nell'Abstract Test Plan

Dal lavoro di analisi critica e comparativa della *Recommendation* richiamato in precedenza, discende l'elenco dei *DTR* che va a comporre l'*ATP*, fornito in allegato, e qui sinteticamente illustrato nella sua struttura complessiva; i numeri tra parentesi indicano le norme della *Recommendation* rilevanti per i requisiti descritti, se seguiti da una lettera indicano che la norma è stata frammentata per una più razionale applicazione e solo parte della stessa quindi è tenuta in considerazione.

Sezione 1 - Requisiti funzionali: garanzia dell'universalità, uguaglianza, libertà e segretezza del suffragio;

1.a) Modalità di espressione del voto (5b, 6, 9, 12, 13, 41, 43, 44, 47, 48, 49, 53, 82, 90a, 91, 96)

1.b) Segretezza del voto (11, 16, 18, 19, 34b, 35, 51, 52, 54, 78, 93a, 103a, 106)

1.c) Trattamento e conteggio dei voti espressi e calcolo dei risultati (5a, 7, 8, 92, 94, 95, 98)

1.d) Usabilità ed accessibilità (14, 50, 61a, 63, 64, 65)

Sezione 2 - Requisiti strutturali: garanzia della corretta progettazione ed implementazione delle misure che conducono alla realizzazione dei requisiti funzionali;

2.a) Hardware: integrità, disponibilità e corretto funzionamento dei sistemi (24, 100a)

2.b) Software: migliori pratiche per la progettazione e codifica (26, 66, 93, 111)

2.c) Osservabilità del corretto funzionamento (23, 56, 83)

Sezione 3 - Requisiti di sicurezza: garanzia della resistenza del sistema ad eventi non accidentali

3.a) Analisi del rischio e misure minime a difesa dalle minacce (14, 20, 27, 28, 29, 69, 76, 77)

3.b) Difesa dei dati memorizzati e trasmessi (75c, 81, 86, 89, 97, 99, 109)

3.c) Accesso al sistema e verifica di conformità (32, 33a, 69b, 72a, 74, 75a, 79a, 80)

3.d) Rilevazione di eventi e reportistica di funzionamento (57, 58, 59, 76, 100b, 101, 102, 103, 104, 107, 108)

Test Plan

Il sistema u-Vote rientra nella categoria dei sistemi di voto online. La redazione del *Technical Data Package* (*TDP*) che lo descrive dettagliatamente è naturalmente a carico del produttore, che lo ha fornito al DWG come da allegato. Utilizzando tale documentazione, si possono trasformare i *DTR* in una raccolta di test specifici che vanno a comporre il *Test Plan*, di seguito riportato limitatamente all'elenco dei test, i cui dettagli sono forniti nel corrispondente allegato.

Sezione 1 - Requisiti funzionali: garanzia dell'universalità, uguaglianza, libertà e segretezza del suffragio;

1.a) Modalità di espressione del voto

- ✓ verifica lista candidati
- ✓ verifica lista elettori
- ✓ verifica impossibilita di modificare le liste
- ✓ verifica ordine sparso lista elezione (randomizzazione ordine rappresentati)
- ✓ verifica richiesta conferma prima di accettare ogni variazione di stato
- ✓ verifica voto
- ✓ verifica non ambiguità delle fasi di voto
- ✓ verifica voto multiplo

1.b) Segretezza del voto

- ✓ verifica della privacy del votante

1.c) Trattamento e conteggio dei voti espressi e calcolo dei risultati

- ✓ verificare dell'adeguata archiviazione dei dati ed in particolare della non cancellabilità
- ✓ verifica del timestamp su ogni ballot
- ✓ verifica sistema di conteggio
- ✓ verifica sistema di conteggio multiplo

1.d) Usabilità ed accessibilità

- ✓ verifica corretta interpretazione delle schermate e del layout

Sezione 2 - Requisiti strutturali: garanzia della corretta progettazione ed implementazione delle misure che conducono alla realizzazione dei requisiti funzionali;

2.a) Hardware: integrità, disponibilità e corretto funzionamento dei sistemi

- Integrità
  - ✓ verifica impossibilità di manipolazione hardware
  - ✓ verifica del processo di boot
  - ✓ verifica impossibilità di aggiungere unità esterne
  - ✓ verifica impossibilità di installare wireless technology

- Disponibilità
  - ✓ verifica robustezza alimentazione (power cord)
  - ✓ verifica allarme e gruppo continuità dell'alimentazione
  - ✓ verifica funzionalità di restore in caso di fault
  - ✓ verifica delle performance della macchina
  - ✓ verifica stress di voto (votazione controllata di votanti multipli)
- Correttezza
  - ✓ verifica degli allacciamenti tra componenti del sistema
  - ✓ verifica della calibrazione dei dispositivi
  - ✓ verifica della precisione temporale

2.b) Software: migliori pratiche per la progettazione e codifica

- verifica della logica del sistema
  - ✓ verifica dei modelli del sistema
  - ✓ verifica della congruenza tra documentazione e implementazione
- readteaming su bugs del codice

2.c) Osservabilità del corretto funzionamento

- ✓ verifica degli indicatori di ON/OFF di "online" o "offline", inchiostro, foglio incastrato nella stampante, ecc.
- ✓ verifica della presenza di un unique ID per software di voto

Sezione 3 - Requisiti di sicurezza: garanzia della resistenza del sistema ad eventi non accidentali

3.a) Analisi del rischio e misure minime a difesa dalle minacce

- Controllo dell'accesso
  - ✓ verifica impossibilita di accesso al SO
  - ✓ verifica procedura di autenticazione (robustezza e durata password)
- Integrità del software
  - ✓ verifica vulnerabilità sistema operativo
  - ✓ verifica presenza di antimalware
  - ✓ verifica signature antimalware
  - ✓ verifica processo di aggiornamento delle signature
  - ✓ verifica funzionamento antimalware e verifica del processo di eliminazione file
  - ✓ verifica periodicità di scanning

3.b) Difesa dei dati memorizzati e trasmessi

- Moduli crittografici:
  - ✓ verifica presenza crittografia in trasmissione e ricezione

- ✓ test algoritmo utilizzato
- ✓ test ambiente di cifratura (dove sono inserite le firme, gli hash ecc.)
- ✓ test robustezza del cifrario
- ✓ test sull'efficacia sistema di generazione di numeri casuali
- ✓ verifica di storing dei dati cifrati

- Firma digitale:
  - ✓ verifica della presenza
  - ✓ verifica della firma apposta ai dati autenticati
  - ✓ test sull'utilizzo della firma
  - ✓ test sull'ambiente (dove sono inserite le firme gli hashes, ecc.)
  - ✓ test sull'efficacia sistema di generazione di numeri casuali
- Comunicazione in rete
  - ✓ verifica delle proprietà di difesa del canale da attacchi di ”uomo nel mezzo”
  - ✓ verifica di limitazione delle comunicazioni al solo dominio del sistema di voto
  - ✓ verifica dei processi che hanno accesso alla rete e del loro funzionamento

3.c) Accesso al sistema e verifica di conformità

- ✓ verifica della completezza della documentazione
- ✓ verifica autorizzazioni per la modifica dei file di configurazione
- ✓ verifica del principio di minimo privilegio
- ✓ verifica impossibilita di aggiungere utenti/gruppi, account lockout
- ✓ verifica dell'impossibilità di modifica del codice non autorizzata

3.d) Rilevazione di eventi e reportistica di funzionamento

- Logging
  - ✓ verifica corrispondenza dei logs agli eventi
  - ✓ verifica identificazione dei log
  - ✓ verifica corretta interpretazione dei log
  - ✓ verificare unicità del formato di log
  - ✓ verificare dell'impossibilità di alterazione del log da parte del software

Conduzione dei test

Ambiente di testing

I test sono stati effettuati presso i Network Security Labs dell'Università degli Studi di Bologna - Seconda facoltà di Ingegneria, con sede a Cesena. Il CINECA ha provveduto personalmente al

trasporto e alla configurazione del sistema di voto all'interno dei laboratori. Tre macchine di proprietà dell'Università sono state connesse al router che collegava la macchina di voto con il server centrale (collocato solo per il test presso il laboratorio). Una macchina chiamata "generatrice" ha svolto il compito di generare il traffico reale al fine di simulare problematiche relative alle problematiche di carico e di concorrenza. Una macchina nominata "Attaccante Diligente" ha svolto il compito di eseguire attacchi mirati al sistema, mentre una macchina denominata "Attaccante Automatico" ha utilizzato software automatici di exploiting e di audit, sia commerciali che open-source.

Metodologia

Considerando la novità sia del sistema, che della procedura di testing sviluppata, la metodologia di testing ha di fatto integrato l'esecuzione dei test veri e propri con la messa a punto di alcuni dettagli del *Test Plan*, che difficilmente avrebbero potuto essere colti in modo appropriato dalla pur rigorosa, ma completamente teorica, analisi fatta tramite i *DTR* ed il *TDP*.

Il flusso di definizione – esecuzione – rapporto dei test, schematizzato in figura 2 il cui contenuto è brevemente chiarito nel seguito, fa riferimento specifico al testing delle caratteristiche di sicurezza, che costituiscono un caso più complesso rispetto alle altre caratteristiche funzionali ed architetturali. È evidente infatti che un *Test Plan* può suggerire le verifiche da compiere per attestare la rispondenza del sistema ai requisiti *minimi* di sicurezza, ma un efficace security testing dipende anche in buona parte dalla capacità di un auditor indipendente di trovare percorsi non ovvi di attacco. Si può considerare questa metodologia un superset più generale di quella comunque adottata per verificare, più semplicemente, la corretta risposta agli stimoli durante i test funzionali.

Define Testing Goals – definire l'obiettivo finale del test; ove per mezzo del *DTR* non sia possibile prevedere tutti gli outcome significativi dei test (come ad esempio nel caso di penetration testing) si provvede a specificare cosa si intende per risultato (nell'esempio, le informazioni raccolte)

Define Objects – definire quale componente è l'oggetto del test, tipicamente questo è chiaro dal *Test Plan*, anche se interazioni e configurazioni non ovvie possono essere l'oggetto di test di sicurezza aggiuntivi.

Posture of the Penetrator – definire quali opportunità di posizionamento e accesso sono disponibili per il tester/attaccante, ad esempio:

- collocazione all'interno o all'esterno del sistema, della rete di comunicazione, ecc.;
- scatola aperta/chiusa: possibilità o meno di modificare il sistema;
- scatola bianca/grigia/nera: grado di visibilità dei dettagli interni del sistema.

Flaw Hypotesis – predisporre un'ipotesi su quali vulnerabilità possono essere presenti.

Find Evidence – definire ed applicare gli Attack Vector (organizzati in Attack Tree) e/o gli stimoli previsti dal *DTR*

Induction Hypotesis – Soprattutto nel caso di security testing, è comune che nuovi obiettivi di test emergano dal comportamento osservato in risposta a stimoli o attacchi, e quindi è opportuno aggiungerli dinamicamente alla lista dei test da effettuare.

Reporting – Documentare dettagliatamente la conduzione del test: corrispondenza tra attività previste dal *Test Plan* ed attività effettivamente condotte, risultati verificati in rapporto a quelli attesi.

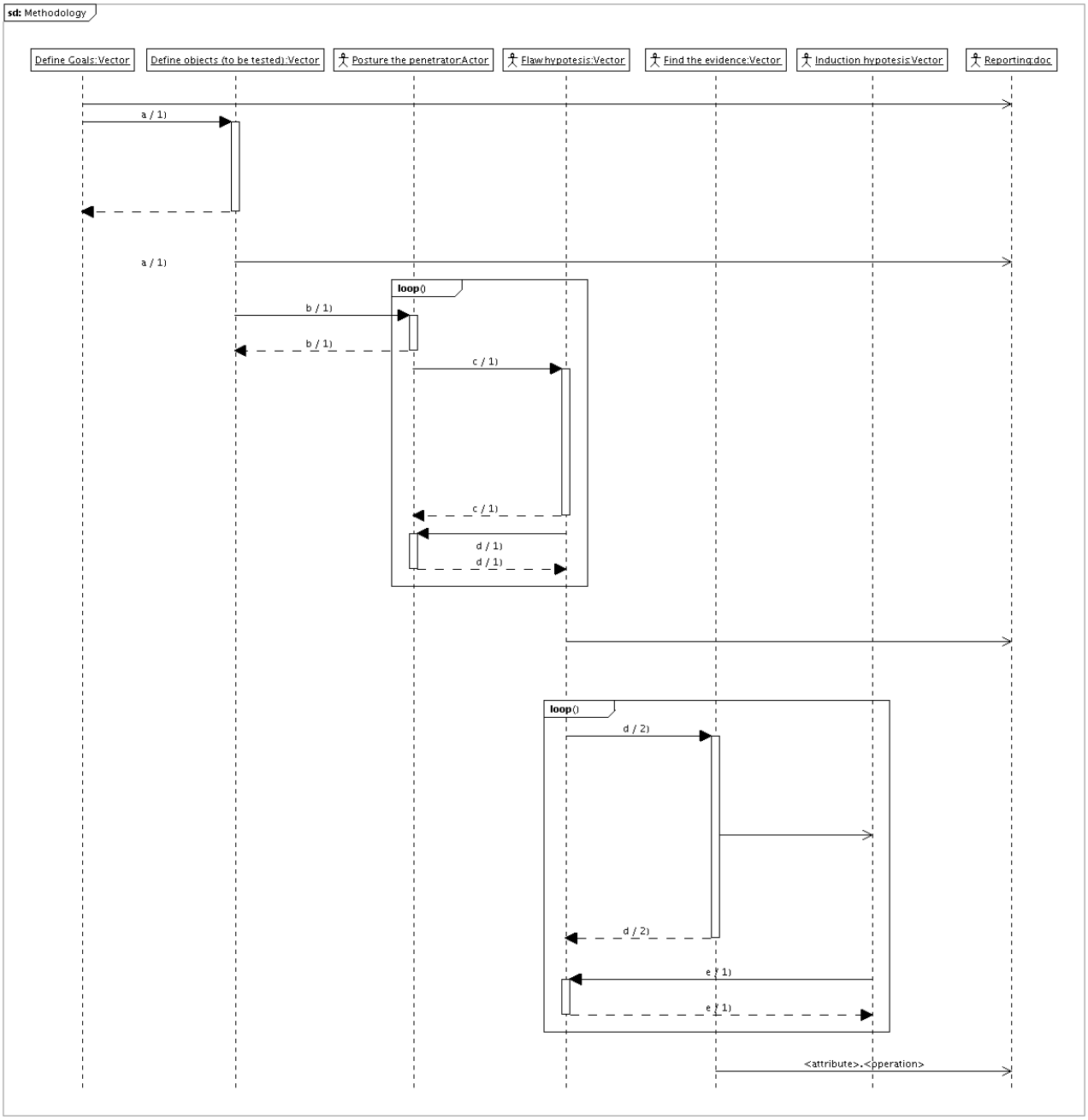

Figura 2 – Metodologia di testing delle caratteristiche di sicurezza

Sintesi dei risultati

I risultati dei test eseguiti secondo i dettami del *Test Plan* sono allegati nel *Test Report*. In questa sede si ritiene opportuno semplicemente richiamare l'attenzione sugli aspetti di particolare sensibilità rilevati, anticipando che:

- tutti i test funzionali sono stati superati,tutti i test strutturali sono stati superati,i test di sicurezza non hanno evidenziato problematiche progettuali e realizzative incongruenti con i prerequisiti specificati dal costruttore.

Il sistema è quindi reputato adatto all'uso per il quale è stato progettato, purché nel rispetto:

- delle ipotesi indicate nella sezione H.4 del TDP, che pongono le precondizioni perché il sistema possa essere considerato sicuro (essenzialmente: la sicurezza fisica e l'integrità del sistema operativo delle postazioni di voto è a carico dell'organizzazione che si avvale del sistema, e non sono quindi previste contromisure addizionali di tipo logico contro potenziali violazioni di tali ipotesi);
- delle raccomandazioni / migliori pratiche riportate nel *Test Report* finale, che individuano dettagliatamente le condizioni ambientali e di configurazione da rispettare per garantire il massimo livello di sicurezza.

Riferimenti

[1] http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Key_Documents/Rec%282004%2911_Eng_Evoting_and_Expl_Memo_en.pdf

[2] http://www.eac.gov/program-areas/voting-systems/voluntary-voting-guidelines/2005-vvsg

[3] Margaret McGaley, J. Paul Gibson, A Critical Analysis of the Council of Europe Recommendations on e-voting. Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop