
Un simulatore per l'analisi del rischio di sicurezza IT in sistemi complessi

Claudio Telmon

Dip. di Informatica
Università di Pisa

Manno, 18 ottobre 2011

Harúspex

Il simulatore è frutto dell'attività del gruppo di ricerca su rischio e sicurezza ICT del Dipartimento di informatica dell'Università di Pisa

- Prof. Fabrizio Baiardi
- Daniele Sgandurra*, Claudio Telmon, Gabriele Piga**

* IIT – CNR – Pisa

** Tesista, laureato con una tesi su Haruspex

Haruspex: indovino etrusco che praticava l'arte divinatoria esaminando i visceri degli animali

Il problema

La sicurezza IT è uno strumento per la gestione del rischio operativo

Il rischio è funzione di impatto e probabilità

→ Semplificando, impatto x probabilità

L'impatto si riesce a stimare

→ Quantomeno, la sua stima è interna all'organizzazione

Ma la probabilità che un agente/minaccia arrivi a provocare quell'impatto?

Scomponiamo il problema

Probabilità di un attacco complesso:

- Caratteristiche della minaccia
- Probabilità che la minaccia attacchi noi
- Probabilità di scoperta delle singole vulnerabilità
- Capacità della minaccia di individuare gli obiettivi
- Capacità della minaccia di praticare attacchi
- Probabilità che i singoli attacchi abbiano successo

Possiamo affrontarli separatamente?

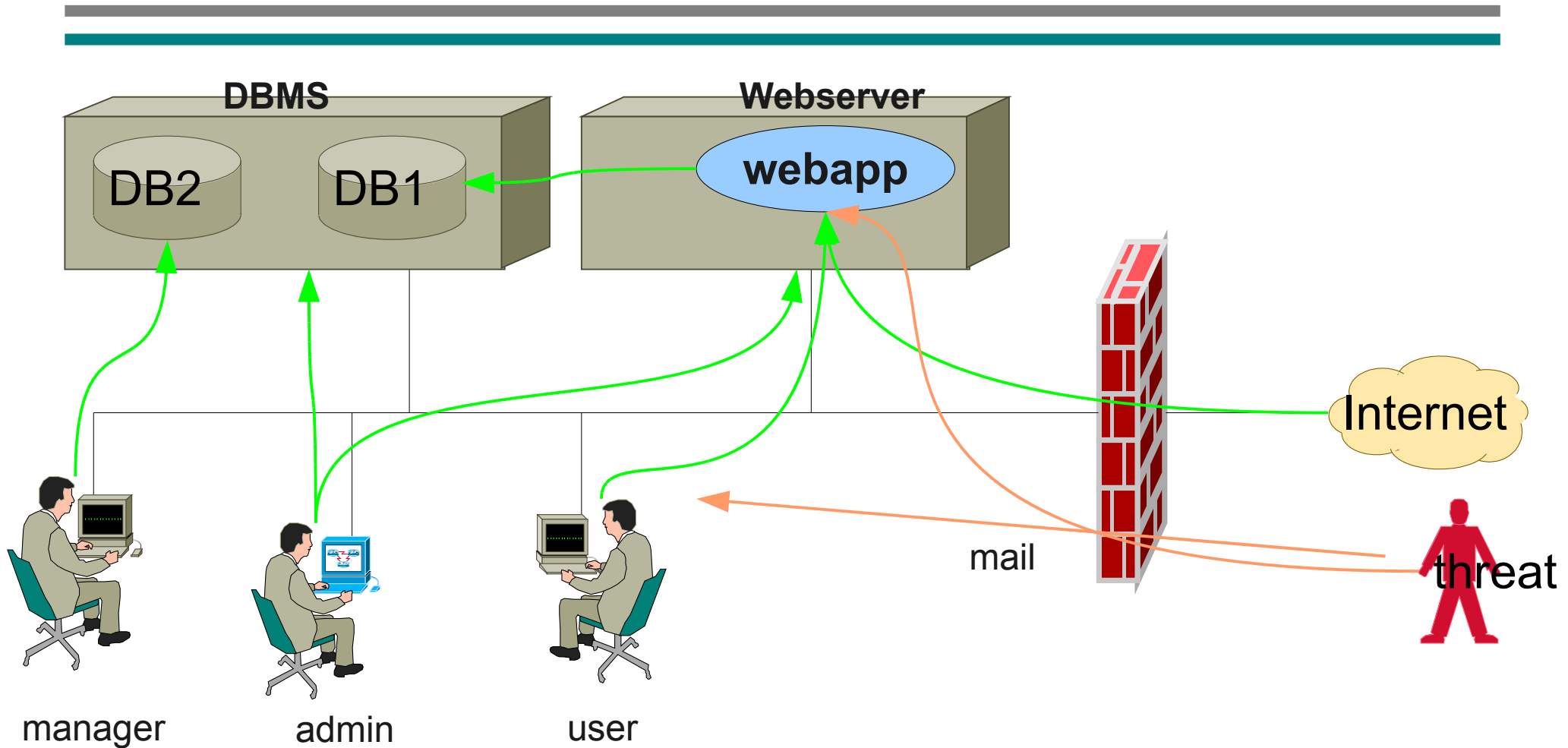
Perché un simulatore

Dobbiamo affrontare un problema complesso, che può essere scomposto in componenti che “interagiscono” fra loro, con una componente probabilistica

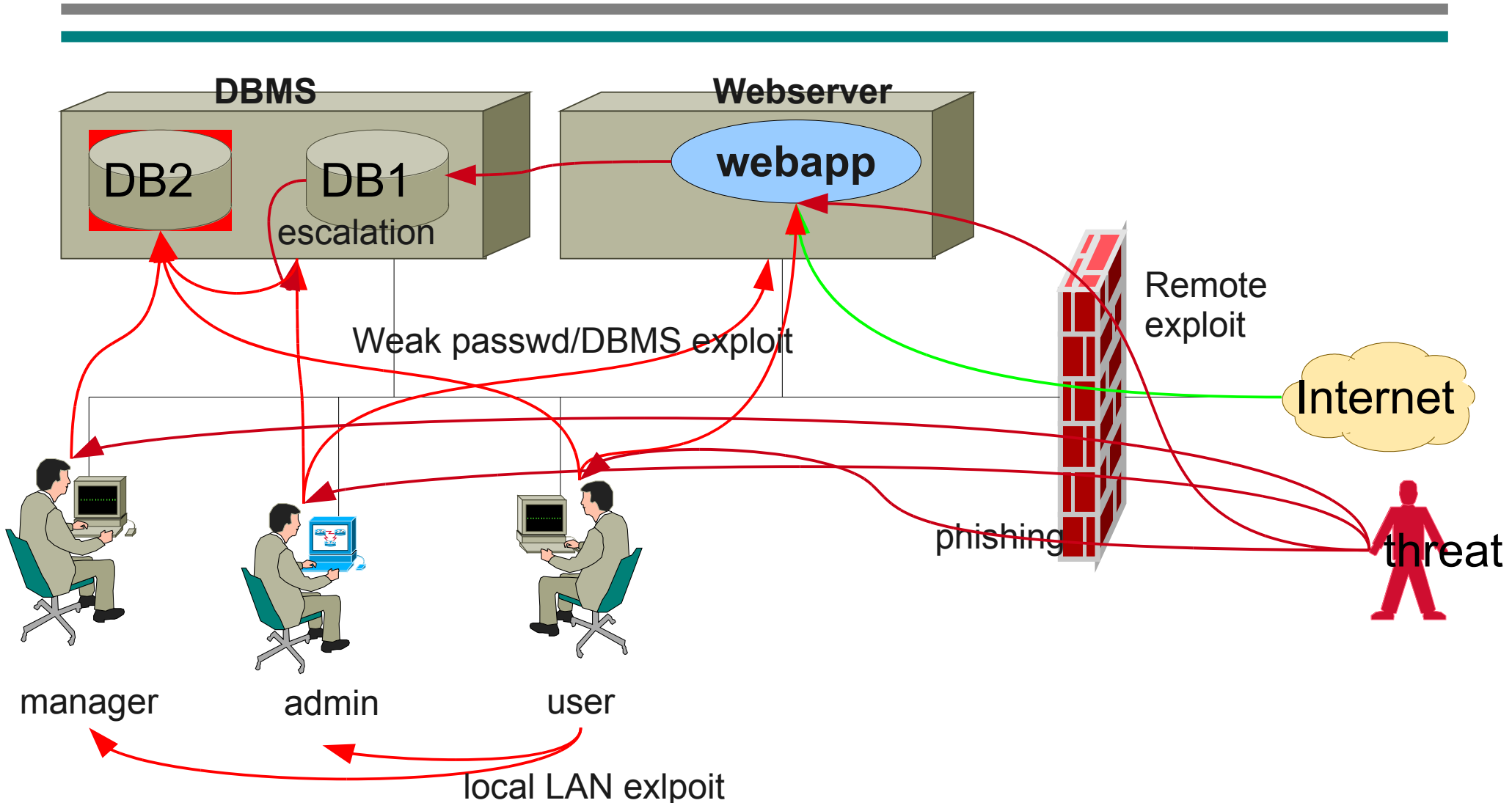
Metodi statistici non parametrici: permettono di fare meno ipotesi sulla popolazione

Metodo Monte Carlo: nasce per lo studio delle particelle (progetto Manhattan)

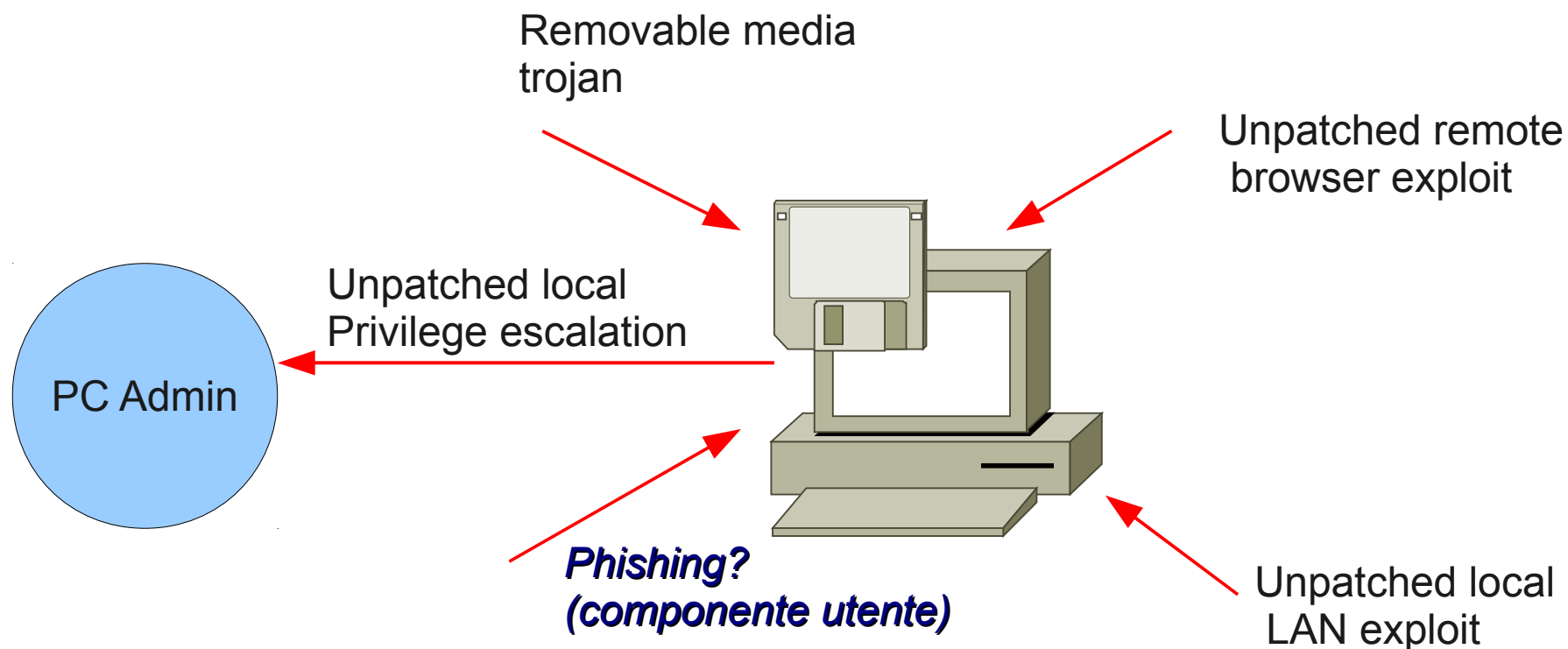
Un sistema



Gli attacchi



Esempio di componente: il PC



Es. chiunque abbia accesso alla rete locale può essere connesso a “unpatched local LAN exploit”

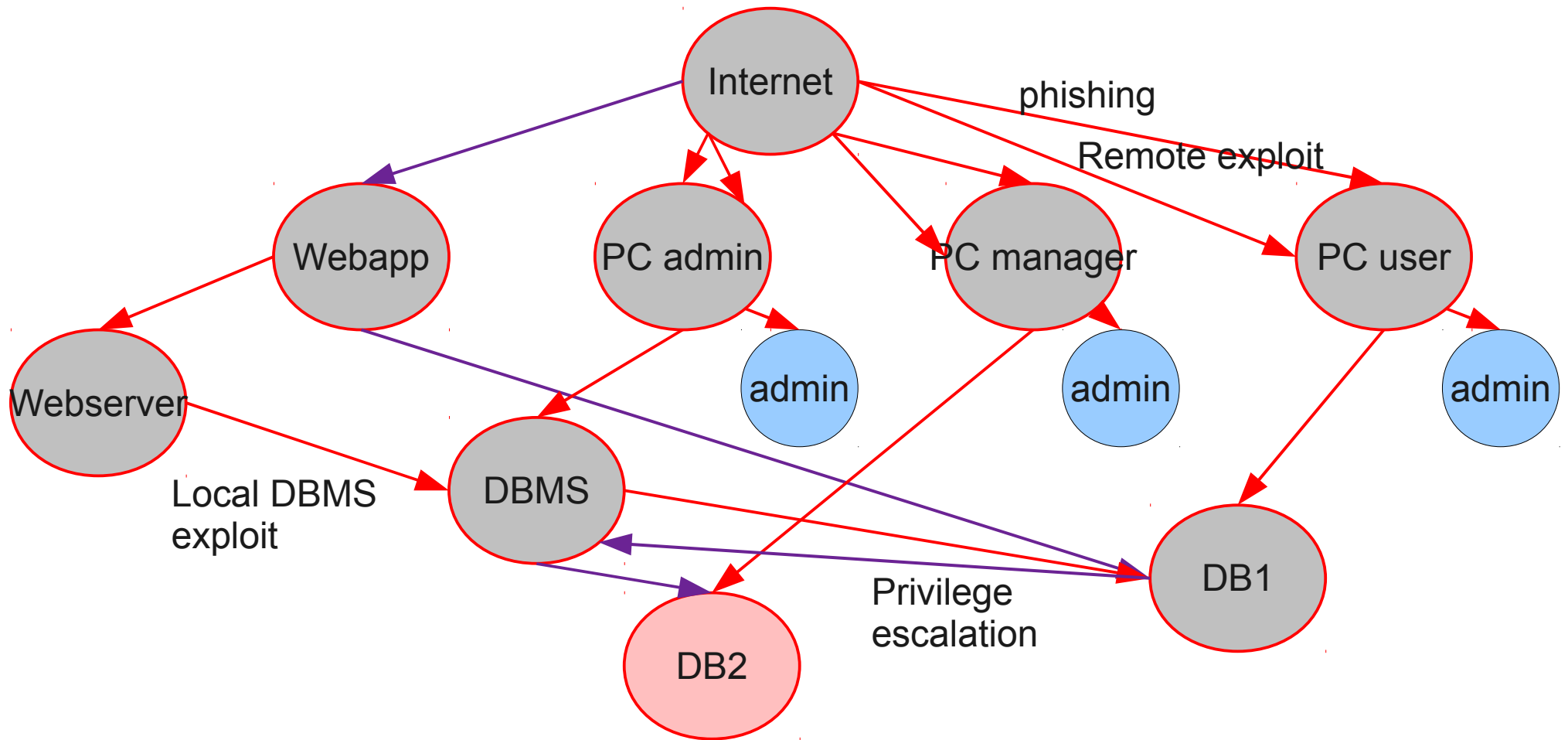
Diritti e dipendenze

Alle operazioni sui componenti sono associati dei ***diritti*** di eseguirle

Una dipendenza fra due operazioni *op1* e *op2* indica che chi ha il diritto di eseguire *op1* ha di fatto il diritto di eseguire *op2*

- Se posso scrivere sul disco, allora posso scrivere sul file (anche se non avrei esplicitamente il diritto di farlo come utente)
- Se posso accedere alla console di un apparato di rete, allora posso leggere il traffico che lo attraversa
 - Il passaggio non sarebbe immediato, ma il modello utilizzato ci permette di non esplicitare tutti i passaggi

Attack graph



Usi e limiti

L'attack graph mi permette di vedere “tutto quello che si può fare”

- Attacco complesso: sequenza di attacchi elementari che mi portano da un insieme di *diritti* iniziale fino ad un *obiettivo*
- L'esempio è molto semplificato: ad esempio, di principio dalla webapp si può attaccare chi la utilizza... un caso reale è molto complesso

Alcuni attacchi sono molto improbabili, quanto ce ne preoccupiamo?

Associamo delle probabilità

- Alle vulnerabilità
- Al successo degli attacchi

Probabilità: un problema locale?

Qual'è la probabilità che in un componente venga scoperta una vulnerabilità **in un certo arco di tempo?**

- Qual'è la probabilità che in un pc Windows venga scoperta una vulnerabilità sfruttabile da remoto nei prossimi sei mesi? Qual'è la finestra di esposizione?
- Risposta: statistiche sui bollettini Microsoft, tempi medi di patching nei nostri sistemi

Riusciamo a dare delle risposte!

Probabilità

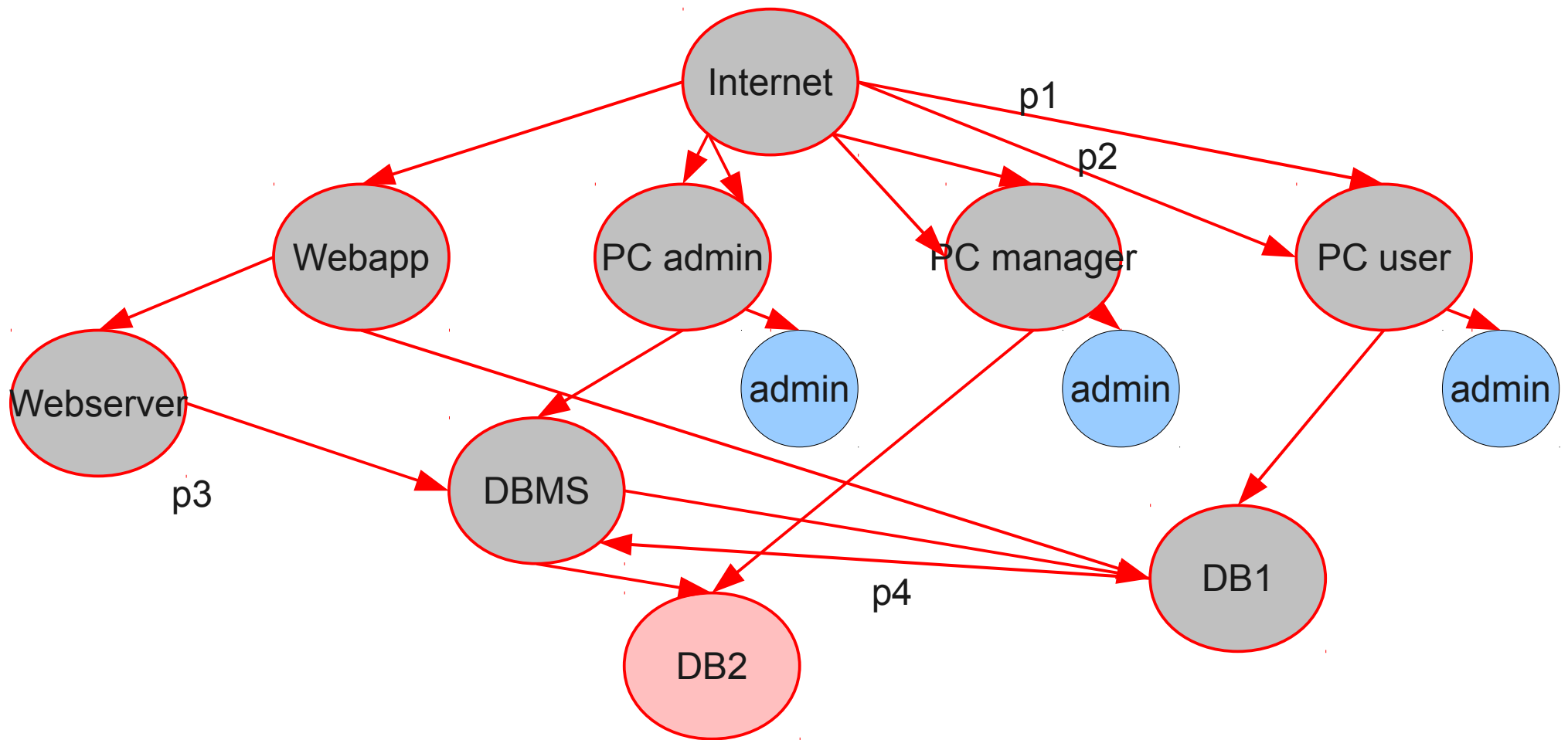
Vulnerabilità

- ➔ Probabilità che un PC presenti nei prossimi sei mesi una vulnerabilità sfruttabile da rete locale
 - Valutabile dalla storia dei bollettini Microsoft (alta)
 - E se i pc sono 1000? Cambia poco – **le probabilità non sono indipendenti**
- ➔ Probabilità che un utente si faccia imbrogliare da una mail ed esegua un programma malevolo?
 - Valutabile con un test sui propri utenti (alta)
 - E se gli utenti sono 1000? Aumenta molto

Attacchi

- ➔ Probabilità che un attacco abbia successo, date le risorse e le competenze necessarie (es. weak password)

Probabilità... ora è ancora più complicato



Soluzione: il simulatore

Negli anni '40, nel corso del progetto Manhattan, per studiare i comportamenti complessi e probabilistici delle particelle, è stato sviluppato il *metodo Monte Carlo*

- Il nome deriva dal Casinò
- Come faccio a sapere qual'è la probabilità che esca una certa combinazione di carte, se per me il problema è matematicamente troppo complesso?
- Risposta: gioco tante partite, e vedo in percentuale quante volte esce quella combinazione
- Più partite gioco, più sono sicuro che statisticamente il risultato sia significativo

Haruspex

Ha in input:

- Una descrizione della minaccia (obiettivi, diritti iniziali, risorse...)
- Una descrizione del sistema
 - Componenti, diritti
 - Vulnerabilità con le loro probabilità
- Una descrizione degli attacchi
 - Diritti: prerequisiti e ottenuti
 - Risorse richieste
 - Probabilità di successo

Esegue più simulazioni indipendenti di attacco e raccoglie dati

La simulazione

Ad ogni step (quanto/unità di tempo):

- Delle vulnerabilità possono essere scoperte
- Le minacce possono tentare attacchi possibili
 - Hanno le risorse, le competenze e la vulnerabilità è stata scoperta; seguono una strategia
 - Se hanno successo, ottengono nuovi diritti da sfruttare allo step successivo
 - Quando la minaccia raggiunge un obiettivo, provoca un impatto

DEMO

Contromisure

Lo scopo ultimo dell'uso di Haruspex è produrre statistiche per individuare le contromisure più efficaci

Una contromisura può:

- ridurre la probabilità di presenza di una vulnerabilità
 - es. migliorare il processo di patch management
- ridurre la probabilità di successo di un attacco
 - es. aumentare la qualità delle password, formare il personale contro il phishing
- modificare l'architettura
 - Introducendo un componente di sicurezza, ad es. un IDS
 - Modificando effettivamente l'architettura

Contromisure per l'esempio

Ridurre i tempi di applicazione delle patch

- Riduce la finestra di esposizione... come?
- Questo mostra la flessibilità del simulatore, perché sia chi gestisce il sistema, sia le minacce possono “eliminare” le vulnerabilità
 - Ad un certo step, con una certa probabilità...

Migliorare la formazione del personale

- Riduce la probabilità di successo di attacchi di phishing

Migliorare la qualità delle password

Ancora contromisure

Comprare un nuovo prodotto di IDS/IPS per il DBMS

Comprare un nuovo prodotto di IDS/IPS per la rete

Implementare una segregazione di rete

- es. attraverso VLAN: i pc degli utenti non comunicano più con quelli dei manager, e non accedono più direttamente al DBMS
- È una vera modifica architetturale
- Si introduce un componente “secure switch” che può avere a sua volta delle vulnerabilità

Security through obscurity:

- Ridurre la diffusione degli indirizzi di posta degli utenti riduce la probabilità di successo del phishing
- Quanto conta per le strategie dell'agente conoscere il sistema?
- Finalmente un dato oggettivo?

Come cambiano le probabilità?

Patch management:

- Prima strada: non cambiano, lasciamo che il simulatore gestisca la finestra di esposizione
- Seconda possibilità: raccogliamo statistiche attraverso i sistemi di patch management sul “prima e dopo” e costruiamo delle metriche

Phishing:

- Test di risposta al phishing prima e dopo le attività di sensibilizzazione

C'è differenza fra 55% e 65% in termini di scelta delle contromisure?

- Anche qui, riusciamo a dare delle risposte quantitative

Cosa cambia negli attacchi?

Simuliamo l'applicazione delle contromisure e misuriamo la riduzione di rischio

- Un vero metodo quantitativo

Le minacce “cambieranno percorso” per arrivare agli obiettivi

- Le nostre contromisure sono efficaci, o hanno solo costretto le minacce a scegliere un'altra strada?

Quali contromisure?

Attraverso il simulatore, scopriamo che:

- Un (costoso) IDS sul DBMS è efficace per gli attacchi che arrivino dal webserver, o attraverso vulnerabilità del DBMS
 - Sono a bassa probabilità
 - Non sono la via di attacco più probabile
 - La riduzione di rischio è bassa, il costo è alto
- Un'attività di sensibilizzazione mirata al management (poche persone)
 - È poco costosa e riduce molto la probabilità...
 - Ma sposta gli attacchi verso gli utenti, che poi attaccano i pc dei manager
- Una soluzione efficace unisce la sensibilizzazione sui manager, buone password ed una segregazione di rete
 - Un IDS di rete potrebbe essere efficace... se si interviene, e rapidamente

Quali punti abbiamo affrontato?

Probabilità di un attacco complesso:

- Caratteristiche della minaccia
- Probabilità che la minaccia attacchi noi
- Probabilità di scoperta delle singole vulnerabilità
- Capacità della minaccia di individuare gli obiettivi
- Capacità della minaccia di praticare attacchi
- Probabilità che i singoli attacchi abbiano successo

E le minacce?

Qual'è la probabilità che una certa minaccia provi ad attaccarci in un certo intervallo di tempo?

- es. qual'è la probabilità che un utente interno cerchi di scaricarsi un database critico nei prossimi sei mesi?
- Qual'è la probabilità che un concorrente cerchi dall'esterno di accedere ai nostri database?

A questo deve rispondere l'organizzazione

- Noi possiamo prendere la risposta come input

Vantaggi di Haruspex

Permette di usare il livello di astrazione preferito

- Anche diverso per componenti diversi
- Dettagliando solo quello che è utile

Permette di rappresentare lo stesso oggetto a diversi livelli nello stesso modello

- Purché siano mantenute le dipendenze
- es. un portatile, il suo disco, un file sul disco

Componenti standard possono essere raccolti in “librerie” da cui attingere

Svantaggi

Il ruolo dell'analista nello scegliere come/quali componenti rappresentare è determinante

- È uno strumento di supporto all'analisi, non di analisi automatica
- I vantaggi si vedono con sistemi complessi

Comunque, non elimina la necessità di “descrivere il sistema”

Valutazione di un sistema

C'è un componente attraverso il quale passano molti degli attacchi di impatto rilevante?

- È un punto debole del sistema

Cosa succede se si introduce una nuova vulnerabilità in un componente?

- Se il rischio aumenta di poco, il sistema è robusto
- Verifica che può essere fatta **in fase di progettazione**

Conclusioni

L'uso di un simulatore permette di ottenere risposte in base a dati o ipotesi locali o comunque elementari e in buona parte ricavabili

- anche grazie alla separazione fra probabilità legate al sistema e probabilità legate alla minaccia

Passiamo da modelli qualitativi camuffati da quantitativi ad un vero modello quantitativo

I risultati sono formalmente verificabili e dimostrabili

Le potenzialità sono molte...

Domande? Feedback?

claudio@di.unipi.it