Analisi dei rischi: esercizi (esercizio 2)

Marco Domenico Aime
< m.aime @ polito.it >

Marco Vallini
< marco.vallini @ polito.it >

Politecnico di Torino
Dip. di Automatica e Informatica

1

Strumenti software

- **modellazione ad alto livello:**
  - Attraverso il linguaggio DFD
  - Attraverso il modello STRIDE
  - Threat Modeling Tool v.3.1
- **risorse:**
  - (home) http://msdn.microsoft.com/en-us/security/dd206731.aspx
  - (tutorial) http://msdn.microsoft.com/en-us/magazine/cc163519.aspx
  - (altre risorse) http://msdn.microsoft.com/en-us/security/cc448120.aspx

2

© Marco Domenico Aime, Marco Vallini (2009)

Workflow

1. **costruzione del modello DFD**
   - a partire dai requisiti descritti di seguito
2. **analisi del modello (suggerimenti del tool)**
   - via metodologia STRIDE
   - aggingere indicazioni sulle possibili contromisure
3. **descrizione dell'ambiente**
   - assunzioni sulla piattaforma software e infrastruttura
   - a partire dai requisiti descritti di seguito
4. **generazione dei report**

3

Contesto

- **l'applicazione PetShop 4.0:**
  - è un'applicazione web
  - permette agli utenti registrati ed anonimi di visualizzare un catalogo elettronico degli oggetti presenti
  - permette agli utenti registrati di ordinare alcuni oggetti appartenenti al catalogo

4

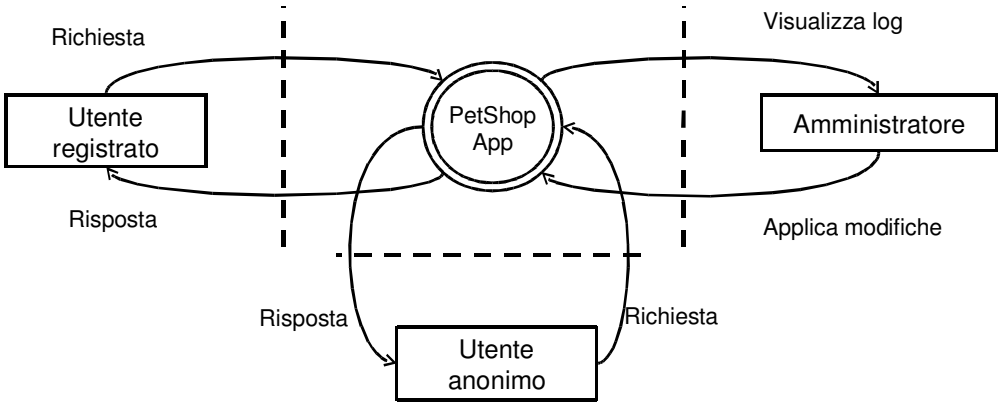
Agenti esterni

- **gli agenti esterni sono di tre categorie diverse:**
  - Utente anonimo
  - Utente registrato
  - Amministratore

5

Processo complesso

- **l'applicazione PetShop può essere rappresentata ad alto livello come un processo complesso**



6

Funzionamento dell'applicazione

- **il processo complesso deve essere scomposto in sotto-processi:**
  - Gestore_Catalogo: processo responsabile di interagire con gli altri processi ed utenti
  - Gestore_Profili: processo per la gestione dei profili utente (creazione nuovi utenti, modifica del profilo, ecc.)
  - Gestore_Ordini: processo per la gestione degli ordini
  - Gestore_Admin: processo utilizzato dall'amministratore per interagire col catalogo, i profili e leggere i dati di audit

7

Funzionamento dell'applicazione

- **Gestore_Catalogo:**
  - interagisce con Processo_Catalogo per:
    - leggere i prodotti contenuti nella base dati del catalogo
  - interagisce con gli utenti

8

Funzionamento dell'applicazione

- **Gestore_Catalogo:**
  - interagisce col processo Gestore_Profili per
    - Creare/aggiornare/leggere i dati relativi
  - interagisce col processo Gestore_Ordini per
    - Creare/aggiornare/leggere i dati relativi

9

Funzionamento dell'applicazione

- **Gestore_Profili:**
  - interagisce con la base dati (Profili) per leggere/creare ed aggiornare i dati relativi ai profili

10

Funzionamento dell'applicazione

- **Gestore_Ordine:**
  - interagisce con la base dati degli ordini (Ordini) per:
    - aggiornare/inserire/leggere un ordine
  - interagisce con Processo_Audit per:
    - registrare le operazioni effettuate sugli ordini
  - Processo_Audit scrive le informazioni all'interno della base dati Audit

11

Funzionamento dell'applicazione

- **Processo_Catalogo:**
  - interagisce con la base dati del catalogo (Catalogo) per:
    - leggere le informazioni sui prodotti

12

Funzionamento dell'applicazione

- **l'amministratore, attraverso Gestore_Admin, può:**
  - leggere i dati di audit (Audit)
  - aggiornare la base dati dei profili degli utenti
  - aggiornare la base dati del catalogo

13

Funzionamento dell'applicazione

- **le informazioni scambiate tra gli utenti ed il Gestore_Catalogo non sono protette con SSL/TLS**
- **le informazioni scambiate tra l'amministratore e il Gestore_Admin sono protette con SSL/TLS**
- **le informazioni scambiate tra i processi sono protette con SSL/TLS e mutua autenticazione attraverso certificati digitali**

14

Funzionamento dell'applicazione

- **le informazioni presenti nelle basi dati possono essere lette e scritte solo previa autenticazione**
- **Gestore_Catalogo utilizza il web server MS IIS ed un software per elaborare le informazioni fornito da terzi**

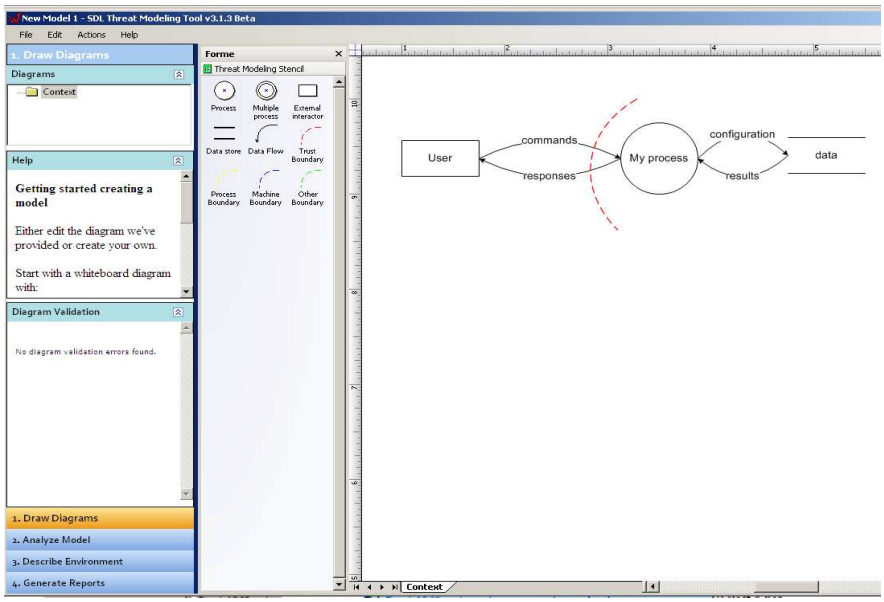
15

Costruzione del modello DFD

- **utilizzando lo strumento Threat Modeling Tool v. 3.1:**
  - costruire il modello DFD all'interno dell'area 'Context'
  - verificare che non vi siano errori di validazione per il modello

16

Costruzione del modello DFD



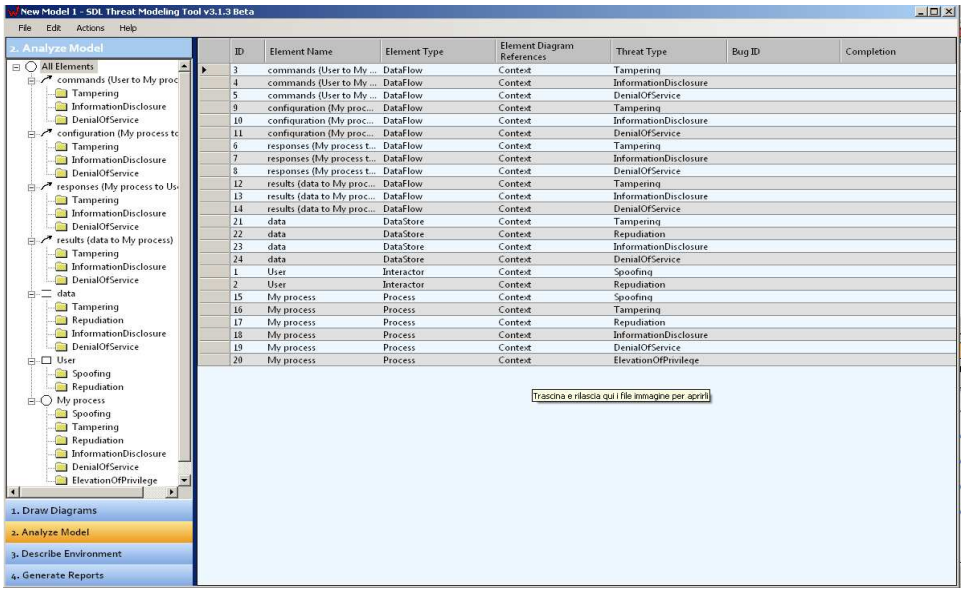
17

Analisi del modello

- **analizzare il modello utilizzando la voce 'Analyze Model'**
- **si aprirà una vista in cui saranno visualizzati:**
  - Interazioni
  - Processi
  - Utenti
  - Dati

18

Analisi del modello



19

Analisi del modello

- **analisi delle categorie di minacce rilevate dallo strumento:**
  - è importante analizzare le diverse categorie per comprendere quali contromisure sono necessarie per annullare o mitigare le minacce
  - è buona norma descrivere le contromisure da adottare

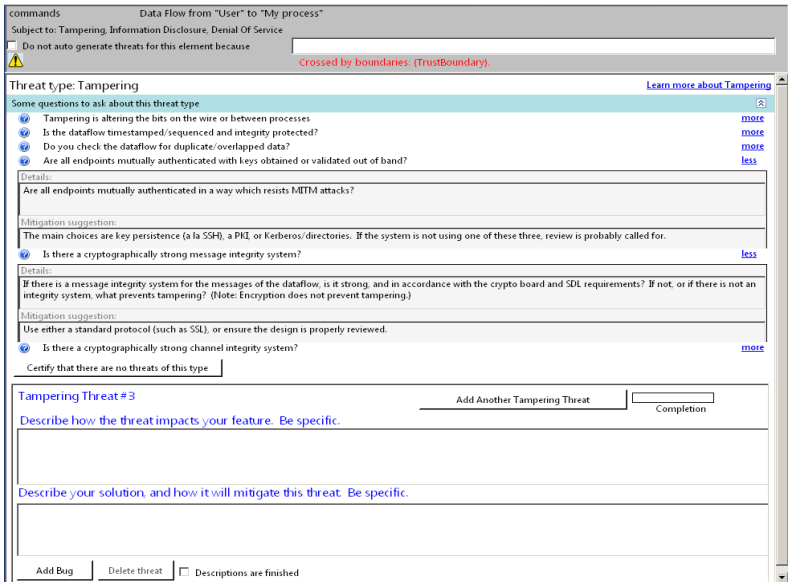
20

Analisi del modello

- **per ciascun elemento (processo, interazione, ecc.):**
  - analizzare le categorie di minacce
    - approccio STRIDE
  - verificare quali contromisure potrebbero essere adottate:
    - il tool fornisce alcuni consigli

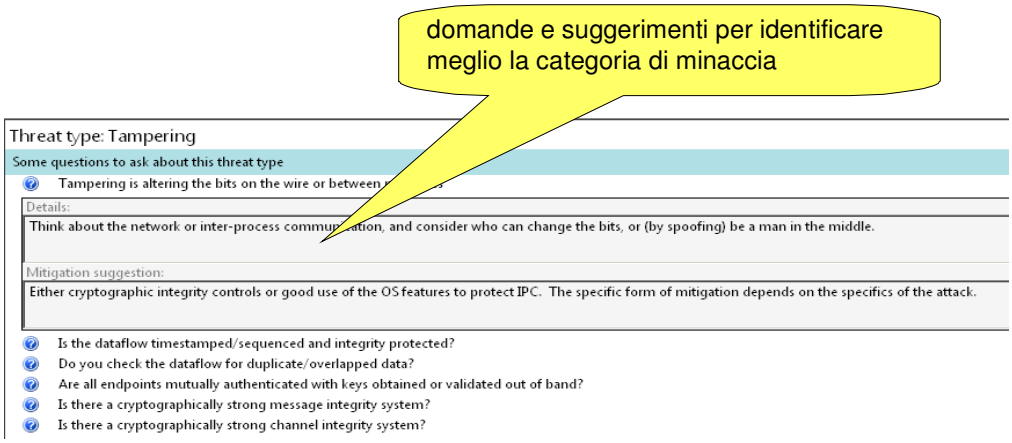
21

Analisi del modello



22

Analisi del modello

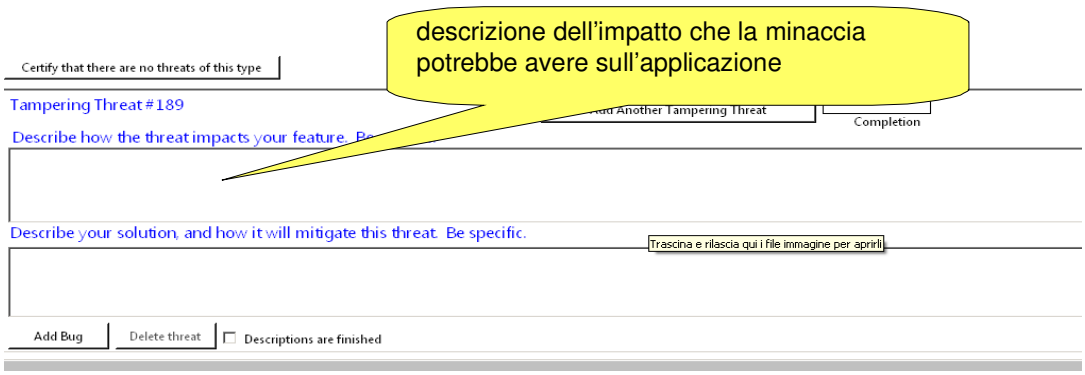


23

Analisi del modello

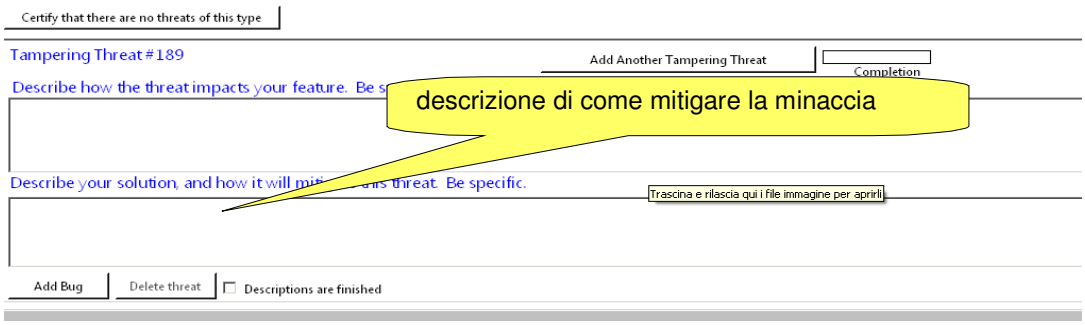
24

Analisi del modello



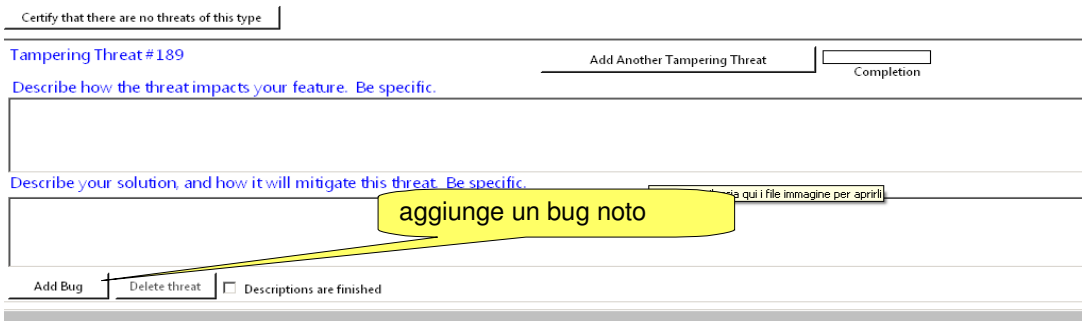
25

Analisi del modello



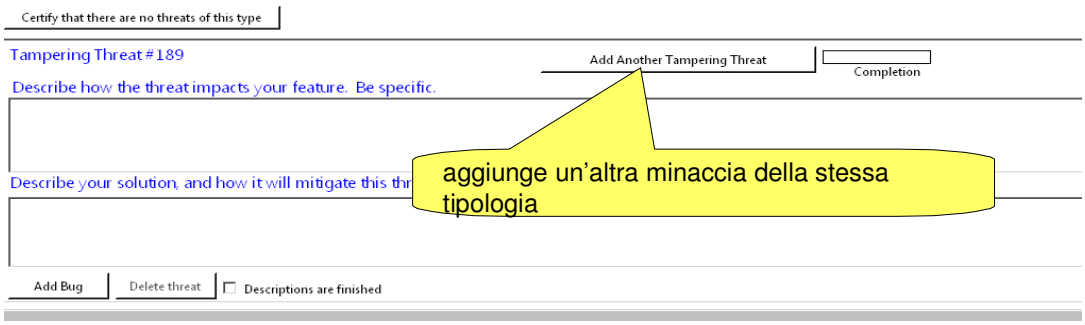
26

Analisi del modello



27

Analisi del modello



28

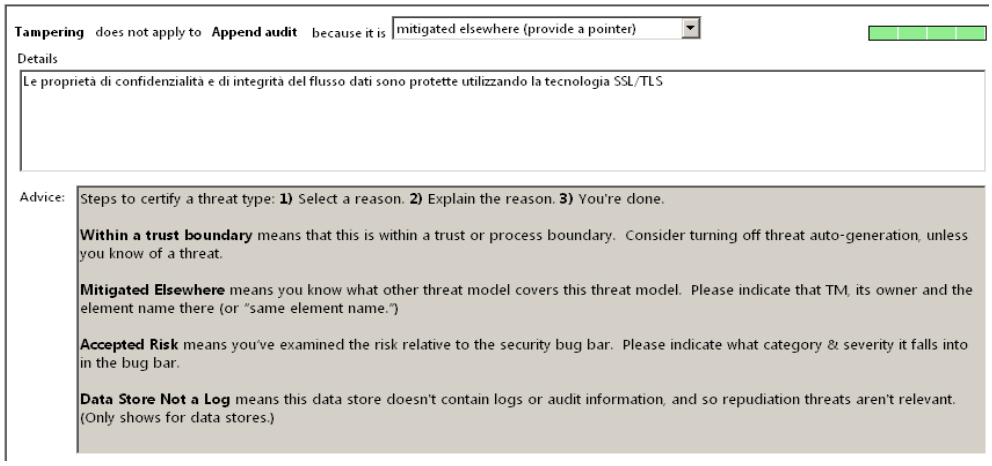
Analisi del modello

- **per ogni categoria di minaccia è possibile:**
  - stabilire che non si applica ad un certo elemento accettando il rischio o fornendo una motivazione:
    - es: per il tampering potremmo utilizzare SSL
  - specificare come si può mitigare una minaccia
  - specificare un particolare bug

29

Analisi del modello

- **utilizzo SSL/TLS per evitare il tampering:**



30

Analisi del modello

- **come esercizio provare ad analizzare e completare le diverse categorie di minacce, evidenziate dallo strumento**
- **per alcune certificare che la minaccia non si applica al sistema, specificando una motivazione**
- **per altre definire come si intende mitigare le problematiche evidenziate**

31

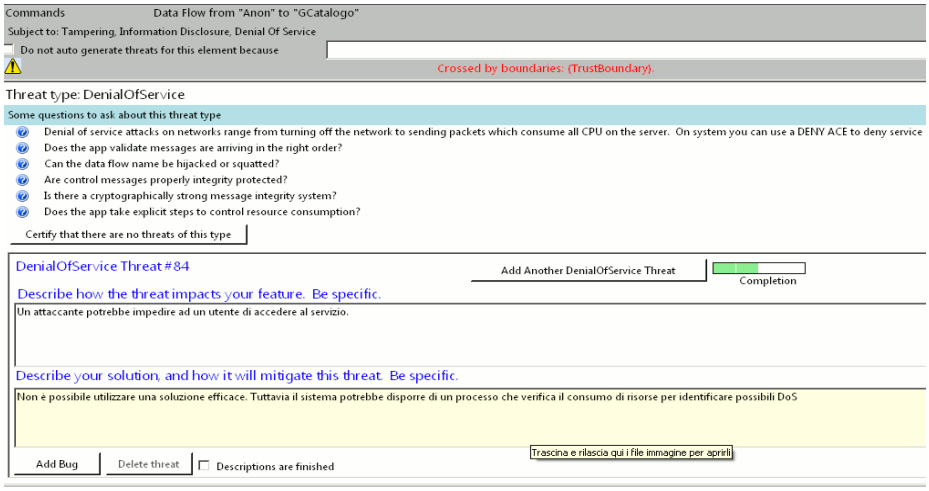
Analisi del modello

- **attacchi DoS verso Gestore_Catalogo:**
  - un attaccante potrebbe eseguire un attacco DoS sul Gestore_Catalogo
  - non è possibile definire contromisure efficaci
  - tuttavia è possibile mitigare la problematica utilizzando un processo che valuti il consumo delle risorse

32

Analisi del modello

- **attacchi DoS verso Gestore_Catalogo:**



33

Analisi del modello

- **Information Discosure per gli archivi:**
  - l'accesso agli archivi potrebbe essere effettuato da diversi processi
  - è necessario prevedere che vi siano meccanismi di autenticazione
  - è consigliabile che vi sia solo un servizio che possa accedere ai dati, che espone delle API per gli altri

34

Analisi del modello

- **Spoofing:**
  - gli utenti registrati possono subire spoofing:
    - è necessario che sia utilizzato un meccanismo di autenticazione
    - è necessario proteggere le credenziali in transito
  - gli utenti anonimo non possono subire spoofing

35

Descrizione dell'ambiente

- **procedere alla descrizione dell'ambiente in cui opera il sistema :**
  - utilizzando la voce 'Describe Environment'

36

Descrizione dell'ambiente

- **esempi di categorie di informazioni da definire:**
  - Gestore_Catalogo utilizza il software MS Windows Server 2003 ed IIS
  - Gestore_Ordini utilizza un web-service sviluppato all'interno dell'organizzazione
  - Gestore_Catalogo è configurato per offrire il servizio esclusivamente attraverso HTTP + SSL/TLS (HTTPS)

37

Descrizione dell'ambiente

- **la descrizione dell'ambiente può essere strutturata in diversi modi:**
  - utilizzando la suddivisione proposta dal tool (assunzioni, dipendenze, ecc.)
  - definendo le caratteristiche come assunzioni

38

Descrizione dell'ambiente

- **la vista permette di classificare le informazioni con le seguenti categorie:**
  - eventuali dipendenze
  - assunzioni circa gli elementi del sistema
  - note di sicurezza per elementi esterni
  - alcune informazioni sul documento

39

Descrizione dell'ambiente

- **dipendenze:**
  - elementi software che interagiscono col sistema ma che non sono descritti nel modello DFD
  - esempio:
    - Gestore_Catalogo utilizza IIS (External)
    - Gestore_Ordini utilizza un servizio sviluppato internamente

40

Descrizione dell'ambiente

- **assunzioni:**
  - utilizzate per descrivere note e considerazioni emerse durante la descrizione del modello del sistema
  - si applicano agli elementi del DFD
  - ad esempio:
    - assumiamo che le il meccanismo di autenticazione presente nel processo principale sia implementato correttamente

41

Descrizione dell'ambiente

- **note di sicurezza per elementi esterni:**
  - considerazioni e note utili per chi deve utilizzare il sistema
  - ad esempio:
    - Il servizio web può essere contattato solo utilizzando il protocollo SSL (HTTPS sulla porta 443)

42

Descrizione dell'ambiente

- **informazioni sul documento:**
  - utili ad individuare il responsabile dell'analisi
  - permette di inserire riferimenti circa:
    - il componente/prodotto software a cui si applica l'analisi
    - quali persone hanno partecipato al processo di analisi (partecipanti e revisori)

43

Generazione del report

- **procedere alla generazione dei report utilizzando la voce 'Generate Reports'**
- **sono disponibili diverse tipologie di report, i più rilevanti per i nostri scopi sono:**
  - Bug Report
  - Analysis Report
  - Threat Model Report

44

Generazione del report

- **Bug Report:**
  - utile per evidenziare tutti i bug specificati durante l'analisi
  - permette di avere una visione globale sulle possibili problematiche di sicurezza introdotte per ciascun componente

45

Generazione del report

- **Analysis Report:**
  - permette di evidenziare rapidamente alcune informazioni circa le analisi condotte, in particolare:
    - quali minacce non sono state trattate dall'analista di sicurezza: ad esempio se non abbiamo preso nessuna decisione per mitigare una problematica
    - le certificazioni e le giustificazioni adottate

46

Generazione del report

- **Threat Model Report:**
  - è il report finale che lo strumento produce
  - contiene informazioni circa:
    - il modello DFD del sistema
    - le diverse categorie di minacce identificate e le soluzioni adottate
    - le dipendenze esterne, assunzioni, ecc.
  - può essere esportato

47

Generazione del report

- **le analisi effettuate evidenziano solo le macro categorie di minacce (STRIDE):**
  - questa analisi è di alto livello e può essere utile al security manager, meno al progettista
- **per le analisi successive considereremo:**
  - l'ultimo report generato
    - Threat Model Report
  - il modello DFD del sistema in esame

48

Soluzione

- **confrontare la soluzione ottenuta con quella fornita nell'esempio allegato**
- **di seguito saranno illustrati gli aspetti più significativi**

49

Soluzione

- **gli utenti anonimi possono leggere le informazioni del catalogo senza autenticarsi:**
  - Spoofing: non applicabile
- **gli utenti registrati possono leggere le informazioni del catalogo ed effettuare ordini, autenticandosi:**
  - Spoofing di identità: le credenziali non sono protette da SSL/TLS, è possibile catturarle e riutilizzarle
  - Contromisura: utilizzare SSL/TLS

50

Soluzione

- **Gestore_Catalogo ed interazioni con gli utenti:**
  - prevede l'autenticazione degli utenti ma questa non è protetta:
    - Spoofing: un attaccante potrebbe sostituire il processo
  - come mitigare la minaccia:
    - proteggere l'autenticazione con SSL/TLS

51

Soluzione

- **Gestore_Admin ed interazioni con gli utenti:**
  - prevede l'autenticazione la mutua autenticazione con utenti ed altri processi, protetta con SSL/TLS e certificati:
    - non è possibile effettuare un attacco di spoofing

52

Soluzione

- **attacchi di tipo DoS:**
  - i processi Gestore_Catalogo e Gestore_Admin e le loro interazioni con l'esterno sono esposti ad attacchi di tipo DoS
  - gli altri processi, interni all'applicazione hanno minore probabilità di soffrire di questo tipo di attacchi:
    - in questo caso l'attacco DoS dovrebbe provenire dall'interno

53

Soluzione

- **attacchi di Tampering sui dati:**
  - le informazioni presenti nelle basi sono accessibili esclusivamente attraverso autenticazione dei dati
  - per modificare i dati è necessario autenticarsi

54

Soluzione

- **attacchi di Repudiation sui dati:**
  - le operazioni sui dati, salvo nel caso degli ordini, non sono registrate:
    - è possibile compiere attacchi di Repudiation
  - contromisura: registrale le operazioni effettuate sui dati

55

Soluzione

- **attacchi di Information Disclosure:**
  - i processi ricevono ed elaborano informazioni da altri processi ed utenti
  - l'elaborazione potrebbe consentire attacchi di Information Disclosure
  - se le elaborazioni sono effettuate da servizi sviluppati all'interno dell'organizzazione e verificati, l'attacco potrebbe essere mitigato

56

© Marco Domenico Aime, Marco Vallini (2009)

Soluzione

- **attacchi di Information Disclosure:**
  - Gestore_Catalogo utilizza:
    - il web server MS IIS
    - le elaborazioni vengono svolte da un software fornito da terzi
  - alcune vulnerabilità potrebbero permettere attacchi di Information Disclosure
  - contromisure: verificare periodicamente bug e vulnerabilità dei software forniti da terzi

57