Descrizione del sistema e Analisi del Rischio

Nicolò Marchi Alessandro Gottoli Mattia Peretti

15 giugno 2012

Indice

1 Descrizione del Sistema

1.1 Panoramica del sistema

L'assegnamento per il laboratorio di Sicurezza delle Reti consisteva nell'implementazione di una Certificate Authority riguardante una fittizia compagnia di nome iMovies, che vuole offrire ai suoi clienti dei servizi basati su PKI (Public Key Infrastructure).

—Possibile descrizione PKI

Il sistema iMovies da noi creato si limita a permettere ad utenti già presenti nel database fornito come materiale allegato al libro Applied Information Security di David Basin, Patrick Schaller e Micheal Schläpfer, la creazione e la firma di certificati che verranno poi usati per la comunicazione sicura tramite e-mail.

L'architettura del sistema consiste in una macchina Ubuntu Server 12.04 con installato il server web Tomcat versione 7. La web application è stata scritta utilizzando il framework Java Server Faces (JSF) per permettere una più facile implementazione visto l'utilizzo del linguaggio Java.

Per la gestione del database ci si è affidati al Relational Database Management System MySql; per la creazione,la firma, la revoca, e tutte le operazioni di gestione dei certificati ci siamo affidati al toolkit OpenSSL, che è un implementazione open-source dei protocolli SSL/TLS.

Per gli archivi di backup dei dati è stato usato il semplice tool tar, presente in ogni distribuzione Unix; per lo scheduling dei backup è stato usato il tool cron, e per il download dei backup ci siamo affidati a

1.2 Funzionalità del Sistema

Innanzi tutto il sistema offre un interfaccia di login per poter accedere al sistema. La fase di login può avvenire attraverso un certificato PKCS#12

1.3 Componenti e Sottosistemi

List all system components, subdivided, for example, into categories such as platforms, applications, data records, etc. For each component, state its relevant properties.

1.4 Interfacce

Specify all interfaces and information flows, from the technical as well as from the organizational point of view.

1.5 Backdoors

Describe the implemented backdoors. **Do not add this section to the version of your report that is handed over to the team that reviews your system!**

1.6 Materiale Aggiuntivo

You may have additional sections according to your needs.

2 Risk Analysis and Security Measures

2.1 Information Assets

Describe the relevant assets and their required security properties. For example, data objects, access restrictions, configurations, etc.

2.2 Threat Sources

Name and describe potential threat sources.

2.3 Risks and Countermeasures

List all potential threats and the corresponding countermeasures. Estimate the risk based on the information about the threat, the threat sources and the corresponding countermeasure. For this purpose, use the following three tables.

Impact	
Impact	Description
High	...
Medium	...
Low	...

Likelihood	
Likelihood	Description
High	...
Medium	...
Low	...

Risk Level			
Likelihood	**Impact**		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

2.3.1 *Evaluation Asset X*

Evaluate the likelihood, impact and the resulting risk, after implementation of the corresponding countermeasures.

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
1	...	...	*Low*	*Low*	*Low*
2	...	...	*Medium*	*High*	*Medium*

2.3.2 *Evaluation Asset y*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
1	...	...	*Low*	*Low*	*Low*
2	...	...	*Medium*	*High*	*Medium*

2.3.3 Detailed Description of Selected Countermeasures

Optionally explain the details of the countermeasures mentioned above.

2.3.4 Risk Acceptance

List all medium and high risks, according to the evaluation above. For each risk, propose additional countermeasures that could be implemented to further reduce the risks.

No. of threat	Proposed countermeasure including expected impact
...	...
...	...