

Contenido

Prefacio	ix
I. Introducción	1
1. Panorama de la seguridad en el Web	3
Seguridad en el Web en pocas palabras	3
El problema de la seguridad en el Web	9
Tarjetas de crédito, encriptación y el Web	14
Firewalls: parte de la solución	20
Administración de riesgos	24
II. Seguridad del usuario	25
2 Errores del navegador: la evolución del riesgo	27
Historia de los navegadores	27
Ataques a través de los datos	33
Fallas de implementación: una letanía de errores	36
3 Java y JavaScript	39
Java	39
JavaScript	54
Ataques de negación de servicio	56
Engaños mediante JavaScript	62
Conclusión	66

4. <i>Descarga de código de máquina mediante ActiveX y plug-ins</i>	67
Cuando los buenos navegadores se vuelven malos	67
Los plug-ins de Netscape	69
ActiveX y el Authenticode	73
Los riesgos de descargar código	77
¿Es el Authenticode una solución?	81
Cómo mejorar la seguridad del código descargado	85
5. <i>Privacía</i>	87
Bitácoras	87
Cookies	90
Información personalmente identificable	94
Anonimizadores	96
Divulgación no anticipada	98
III. <i>Certificados digitales</i>	99
6. <i>Técnicas de identificación digital</i>	101
Identificación	101
Infraestructura de llaves públicas	112
Problemas con la construcción de una infraestructura de llaves públicas	119
Diez preguntas sobre políticas	126
7. <i>Autoridades certificadoras y certificados de servidores</i>	132
Los certificados hoy	132
Certificados de autoridades certificadoras	134
Certificados de servidores	137
Conclusión	150
8. <i>Certificados digitales para los clientes</i>	151
Certificados de clientes	151
Una visita al Centro de Identificación Digital de VeriSign	153
9. <i>Firmas de código y el Authenticode de Microsoft</i>	169
¿Por qué firmar el código?	169
La tecnología Authenticode de Microsoft	172
Cómo obtener un certificado de editor de software	181
Otros métodos de firma de código	182

IV. Criptografía	185
10. Introducción a la criptografía	187
Qué es la criptografía	187
Algoritmos de llaves simétricas	193
Algoritmos de llaves públicas	200
Funciones de compendio de mensajes	202
Infraestructura de llaves públicas	207
11. La criptografía y el Web	209
La criptografía y la seguridad en el Web	209
Los sistemas actuales de encriptación	212
Restricciones estadounidenses sobre la criptografía	219
Restricciones de otros países sobre la criptografía	229
12. Los protocolos SSL y TLS	233
Qué es SSL	233
Actividades del estándar TLS	243
SSL: El punto de vista del usuario	243
V. Seguridad de servidores web	251
13. Seguridad de la máquina y del sitio	253
Máquinas históricamente inseguras	253
Principales problemas de seguridad de las máquinas hoy día	255
Cómo reducir el riesgo minimizando servicios	268
Actualización segura del contenido	270
Bases de datos traseras	272
Seguridad física	273
14. Control de acceso al servidor web	275
Estrategias de control de acceso	275
Control de acceso mediante bloques <Limit>	280
Un sistema sencillo de administración de usuarios	286
15. Programación segura con CGI y API	293
El peligro de la extensibilidad	293
Reglas para codificar	300
Reglas específicas para lenguajes de programación específicos	305

Consejos para escribir programas de CGI que se ejecuten con privilegios adicionales	308
Conclusión	309
VI. Comercio y sociedad	311
16. Pagos digitales	313
Charga-Plates, Diners Club y las tarjetas de crédito	313
Sistemas de pago basados en Internet	322
Cómo evaluar un sistema de pagos mediante tarjeta de crédito	332
17. Software de bloqueo y tecnología de censura.....	335
Software de bloqueo	335
PICS	338
RSAGi	346
18. Consideraciones legales: civiles.....	349
Propiedad intelectual	350
Demandas	359
19. Consideraciones legales: penales.....	362
Opciones legales tras una irrupción	362
Peligros penales que pueden esperarle	367
Material delictivo	370
Juegue a la segura.....	372
Las leyes y el activismo	374
VII. Apéndices.....	377
A. Lecciones de Vineyard.NET.....	379
B. Creación e instalación de certificados de servidores web.....	402
C. El protocolo SSL 3.0	417
D. La especificación de PICS	442
E. Referencias	453
Índice	471