Prefazione alla nuova edizione

La maggior parte dei libri spiega che cos'è la crittografia, quali sono gli schemi attuali e come funzionano i protocolli crittografici esistenti, come SSL/TLS. Il precedente libro di Bruce Schneier, *Applied Cryptography*, è uno di questi. Questi libri forniscono utilissimi riferimenti per chiunque lavori con la crittografia, ma si mantengono a un passo di distanza dalle esigenze concrete dei crittografi e dei tecnici della sicurezza. A chi si occupa di crittografia e di sicurezza non basta sapere come funzionano i protocolli crittografici attuali, devono sapere come utilizzare la crittografia, e per raggiungere questo scopo è necessario imparare a pensare come un professionista del campo.

Questo libro è stato pensato per aiutarvi a raggiungere tale scopo, utilizzando la strategia dell'immersione: anziché discutere ampiamente i protocollo che potreste incontrare nella crittografia, ci addentreremo profondamente nella progettazione e nell'analisi di protocolli specifici, utilizzati nella pratica. Vi condurremo per mano nella progettazione di protocolli crittografici, condividendo con voi i motivi per cui preferiamo determinate scelte rispetto ad altre ed evidenziando le insidie presenti lungo la strada.

Imparando a pensare come un professionista della crittografia, imparerete anche a diventare un utente più perspicace. Sarete in grado di esaminare i toolkit crittografici disponibili, di capirne le funzionalità centrali e di utilizzarli al meglio. Capirete meglio anche le sfide della crittografia e come tentare di superarle.

Questo libro serve anche per introdurvi al campo della sicurezza informatica.

La sicurezza informatica è per molti aspetti una sovrainsieme della crittografia. Entrambe le discipline trattano la progettazione e la valutazione di oggetti (sistemi o algoritmi) pensati per comportarsi in determinati modi anche in presenza di un avversario. In questo libro imparerete a pensare all'avversario nel contesto della crittografia. Quando avrete imparato a pensare come il nemico, potrete applicare tale mentalità al campo della sicurezza informatica in generale.

Evoluzione del libro

La prima edizione di questo libro, con il titolo *Practical Cryptography*, è stata scritta da Niels Ferguson e Bruce Schneier. In seguito agli autori si è aggiunto Tadayoshi Kohno – Yoshi per gli amici. Yoshi è professore di Computer Science and Engineering all'Università di Washington e in passato è stato collega di Niels e Bruce; ha lavorato su

Practical Cryptography per adattarlo all'utilizzo in corsi collettivi e per lo studio personale, mantenendo sempre validi gli obiettivi e i temi fondamentali del libro originale scritto da Niels e Bruce.

Percorsi didattici di esempio

Questo libro può essere letto in vari modi. Potete utilizzarlo come guida di autoapprendimento per la crittografia applicata, oppure in un normale corso di studio. All'interno di un corso semestrale di sicurezza informatica, il libro potrebbe servire da base per un percorso intensivo di sei settimane dedicato alla crittografia. Oppure potrebbe costituire il riferimento di un corso semestrale sulla crittografia, eventualmente con l'aggiunta di materiali più avanzati qualora il tempo lo consenta. Per facilitarne l'utilizzo nei corsi di studio, presentiamo di seguito alcuni possibili percorsi didattici.

Il syllabus che segue è adatto per un percorso intensivo di 6 settimane sulla crittografia. Presupponiamo in questo caso che il contenuto del Capitolo 1 sia trattato separatamente, nel contesto più ampio della sicurezza informatica.

Settimana 1: Capitoli 2, 3 e 4

Settimana 2: Capitoli 5, 6 e 7

Settimana 3: Capitoli 8, 9 e 10

Settimana 4: Capitoli 11, 12 e 13

Settimana 5: Capitoli 14, 15, 16 e 17

Settimana 6: Capitoli 18, 19, 20 e 21

Il syllabus che segue è adatto per un percorso trimestrale di 10 settimane sulle tecniche crittografiche.

Settimana 1: Capitoli 1 e 2

Settimana 2: Capitoli 3 e 4

Settimana 3: Capitoli 5 e 6

Settimana 4: Capitoli 7 e 8

Settimana 5: Capitoli 9 e 10

Settimana 6: Capitoli 11 e 12

Settimana 7: Capitoli 13 e 14

Settimana 8: Capitoli 15, 16 e 17

Settimana 9: Capitoli 18, 19, 20

Settimana 10: Capitolo 21

Il syllabus che segue è adatto per corsi semestrali di 12 settimane. Può anche essere esteso con materiali avanzati sulla crittografia o la sicurezza informatica, per periodi più lunghi.

Settimana 1: Capitoli 1 e 2

Settimana 2: Capitoli 3 e 4

Settimana 3: Capitoli 5 e 6

Settimana 4: Capitolo 7

Settimana 5: Capitoli 8 e 9
Settimana 6: Capitoli 9 (continua) e 10
Settimana 7: Capitoli 11 e 12
Settimana 8: Capitoli 13 e 14
Settimana 9: Capitoli 15 e 16
Settimana 10: Capitoli 17 e 18
Settimana 11: Capitoli 19 e 20
Settimana 12: Capitolo 21

Il libro contiene diversi tipi di esercizi e incoraggiamo i lettori a svolgerne il più possibile. Ci sono esercizi tradizionali progettati per verificare la comprensione degli aspetti tecnici della crittografia. Tuttavia, poiché il nostro scopo è quello di aiutarvi a imparare come pensare alla crittografia nel contesto di sistemi reali, abbiamo introdotto anche alcuni esercizi non tradizionali (cfr. Paragrafo 1.12). La crittografia non è un mondo isolato, ma fa parte di un ecosistema più ampio, costituito da altri sistemi hardware e software, persone, economia, etica, differenze culturali, politica, legislazione e così via. I nostri esercizi non tradizionali sono progettati proprio per costringervi a pensare alla crittografia nel contesto di sistemi reali e dell'ecosistema che li circonda. Questi esercizi vi forniranno l'opportunità di applicare direttamente i contenuti del libro come esercizi di riflessione sui sistemi reali. Inoltre, intrecciando insieme gli esercizi in tutto il libro, sarete in grado di vedere come crescono le vostre conoscenze mentre progredite nella lettura capitolo dopo capitolo.

Informazioni aggiuntive

Nonostante tutti gli sforzi profusi nella revisione del libro, qualche errore sarà certamente presente. È disponibile online un elenco di *errata* presso il sito di Bruce Schneier, utilizzabile nel modo seguente.
Prima di leggere questo libro, collegatevi a `http://www.schneier.com/ce.html` e prelevate l'elenco di correzioni aggiornato.
Se trovate un errore nel libro, verificate se è già citato nell'elenco. Se non lo è, segnalatelo via email a `cryptographyengineering@schneier.com`. Lo aggiungeremo all'elenco.
Vi auguriamo uno splendido viaggio nel mondo della crittografia. Il tema è bellissimo e affascinante. Speriamo che possiate imparare molto da questo libro e arrivare ad amare la crittografia come l'amiamo noi.

Ottobre 2009

Niels Ferguson
Redmond, Washington
USA
`niels@ferguson.net`

Bruce Schneier
Minneapolis, Minnesota
USA
`schneier@schneier.com`

Tadayoshi Kohno
Seattle, Washington
USA
`yoshi@cs.washington.edu`