Segurança de Aplicativos Android

Jeff Six

Novatec

Editor: Rubens Prates
Tradução: Eduardo Kraszczuk
Revisão técnica: João Paulo Lemos Escola
Revisão gramatical: Patrizia Zagni
Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-313-0

Histórico de impressões:

Junho/2012 Primeira edição

Novatec Editora Ltda.
Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
Fax: +55 11 2950-8869
Email: novatec@novatec.com.br
Site: www.novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Six, Jeff
Segurança de aplicativos Android /
Jeff Six ; [tradução Eduardo Kraszczuk].
-- São Paulo : Novatec Editora ; Sebastopol,
CA : O'Reilly, 2012.

Título original: Application security for the
Android Platform.
ISBN 978-85-7522-313-0

1. Android (Programa de computador) - Medidas
de segurança 2. Aplicação de programas -
Desenvolvimento 3. Computação móvel I. Título.

12-06640 CDD-005.26

Índices para catálogo sistemático:

1. Android : Plataforma de desenvolvimento para
aplicativos móveis : Programa de computador
005.26

Sumário

Sobre o autor **9**

Prefácio **11**

Organização do livro 11
Convenções usadas neste livro 12
Uso dos exemplos de códigos de acordo com a política da O'Reilly 13
Como entrar em contato conosco 14
Agradecimentos 14

Capítulo 1 ■ Introdução **15**

Segurança de aplicativos: por que você deveria se importar com isso? 16
Estado atual da segurança de aplicativos móveis no Android 18
Segurança: risco = vulnerabilidade + ameaça + consequências 20
Evolução da segurança da informação: por que os aplicativos são o mais importante 23
Sua função: proteger os dados 24
Técnicas de desenvolvimento de software seguro 25
Características únicas do Android 27
Prosseguindo 30

Capítulo 2 ■ Arquitetura Android **31**

Introdução à arquitetura Android 32
Modelo de segurança Linux 33
Modelo de segurança Android resultante 34
Assinatura, atribuição e atestação de aplicativo 35
Design de processo 38
Isolamento do sistema de arquivos Android 41
Preferências Android e isolamento de base de dados 44
Subindo as camadas até as APIs de sistema e permissões de componente 45

Capítulo 3 ■ Permissões de aplicativo 47

Básico das permissões no Android 50
Usando APIs de sistema restritas e a experiência de usuário 52
Permissões personalizadas 56

Capítulo 4 ■ Segurança e permissões de componente 61

Tipos de componentes Android 61
Sinalização intercomponente usando intents 63
Componentes públicos e privados 66
Impondo restrições ao acesso a componentes 67
    Protegendo Activitys 68
    Protegendo services 68
    Protegendo Content Providers 70
    Protegendo Broadcast Intents 77
Reunindo tudo: protegendo comunicações em um app multicamada 79

Capítulo 5 ■ Protegendo dados armazenados 83

Ameaças e vulnerabilidades contra dados armazenados 83
    Vulnerabilidades dos dados armazenados 84
    Ameaças e mitigações para dados armazenados 85
Princípios de proteção 86
Cartilha da criptografia: encriptação 87
    Encriptação simétrica 87
    Encriptação de chave assimétrica 89
    Cartilha da criptografia: hashing 90
Aspectos práticos da criptografia 92
    Inviabilidade computacional 93
    Escolha do algoritmo e tamanho da chave 93
    Modos de operação de cifra, vetores de inicialização e salt 94
    Chaves públicas e seu gerenciamento 95
Derivação e gerenciamento de chave 97
    Motivação 97
    Derivação de chave 98
    Encriptação sem derivação de chave fornecida pelo usuário 102
Criptografia prática: aplicando uma técnica contra uma ameaça 103

Capítulo 6 ■ Protegendo interações de servidor 109

Confidencialidade e autenticação 109
SSL/TLS: o padrão da indústria 110
    Autenticação das entidades 111

Encriptação de dados ... 113
Protegendo dados em transmissão para serviços públicos ... 114
Apresentando o ambiente SSL/TLS no Android ... 114
Verificação de servidor ... 115
Lidando com erros de conexão SSL/TLS ... 118
Protegendo dados em tráfego para serviços privados ... 120
Usando somente certificados específicos para o SSL/TLS ... 120
Um passo além: usando autenticação SSL/TLS do lado do cliente ... 125
Ameaças contra dispositivos usando dados em trânsito ... 128
Validação de entrada: o principal elemento da segurança de aplicativo ... 131
Rejeitar o que sabemos ser ruim ... 131
Aceitar o que sabemos ser bom ... 132
Resumindo: validação de entrada ... 133
Impedindo a injeção de comandos ... 133

Capítulo 7 ■ Sumário ... 137

Temas principais ... 137
É tudo sobre risco ... 137
Princípio do Privilégio Mínimo ... 138
Use o sistema de permissões ... 138
O Android é uma arquitetura aberta ... 138
Acerte na criptografia ... 139
Nunca confie nas entradas de usuário ... 139
Encerrando ... 139