



IME - Instituto de
Matemática e Estatística

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

Implementando protocolos de acordo de chave baseados em identidade e sem certificado na plataforma Android

Rafael Will Macedo de Araujo

rwill@ime.usp.br

<http://www.ime.usp.br/~rwill>

DCC – IME – USP

11 de Setembro de 2012

CNPq no. 151134/2010-3





IME - Instituto de
Matemática e Estatística

Objetivos

Seminário de Segurança de Dados e Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Revisão dos conceitos de criptografia de chave pública baseada em identidades e sem certificado.
- Introduzir as ferramentas básicas para construção de código nativo na plataforma *Android*.
- Expor nossa proposta de pesquisa.
- Mostrar os resultados parciais obtidos.



IME - Instituto de
Matemática e Estatística

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

Protocolos de Acordo de Chave

Problema

Como duas pessoas podem combinar uma chave secreta sem necessidade de um encontro?

Solução

Através de um protocolo de acordo de chaves.

- Acordo de chave é o processo no qual dois ou mais participantes combinam uma chave secreta, de modo que ambos influenciam no resultado.

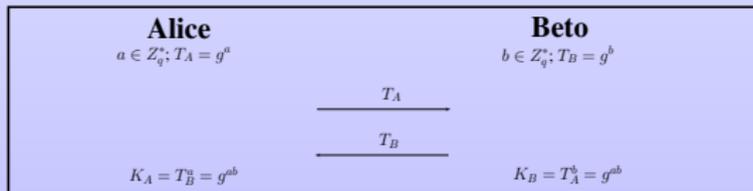


Figura: Acordo de chave Diffie-Hellman (1976)

Criptografia de Chave Pública Baseada em Identidade



IME - Instituto de
Matemática e Estatística

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Modelo proposto em 1984, por Adi Shamir.
- A chave pública deixa de ser um valor gerado aleatoriamente, e passa ser a própria **identidade do usuário**.
 - Exemplos: *nome, e-mail, CPF, n° de telefone, endereço IP, etc.*
- Pressupõe a existência de um **Gerador de Chaves Privadas** (PKG - *Private Key Generator*).
 - Responsável por: gerar e guardar a chave-mestra secreta, calcular chaves privadas de todos os usuários, entregar as chaves privadas dos usuários de forma segura.



IME - Instituto de
Matemática e Estatística

Diagrama do Modelo Baseado em Identidade

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

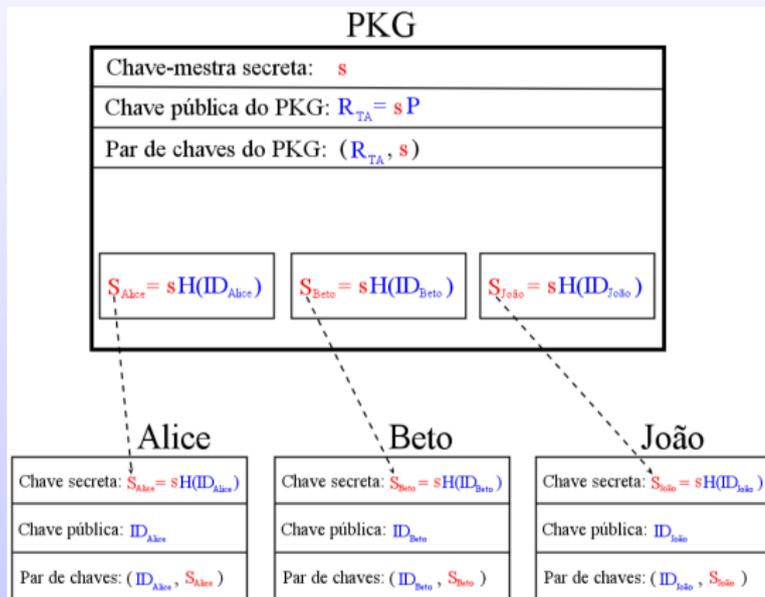


Figura: Distribuição das chaves privadas no modelo baseado em identidade



IME - Instituto de
Matemática e Estatística

Seminário de Segurança de Dados e Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

Criptografia de Chave Pública sem Certificado

- Modelo proposto em 2003 por S. Al-Riyami e K. Paterson.
- Combina as ideias do modelo baseado em identidades com o modelo de chave auto-certificada (proposto por Girault em 1991).
 - Um dos principais objetivos era eliminar a propriedade de custódia de chaves, inerente ao modelo baseado em identidade.
- Trata-se de um modelo intermediário entre o baseado em identidade e a ICP.
- Pressupõe a existência de uma Autoridade de Confiança, chamada de KGC (*Key Generation Center*).
 - Responsável por: gerar e guardar a chave-mestra secreta, calcular **chaves secretas parciais** de todos os usuários, entregar as **chaves secretas parciais** dos usuários de forma segura.



IME - Instituto de Matemática e Estatística

Diagrama do Modelo sem Certificado

Seminário de Segurança de Dados e Criptografia

Rafael Will M. de Araujo

Objetivos

Introdução

Desenvolvendo para Android

Proposta

Resultados Parciais

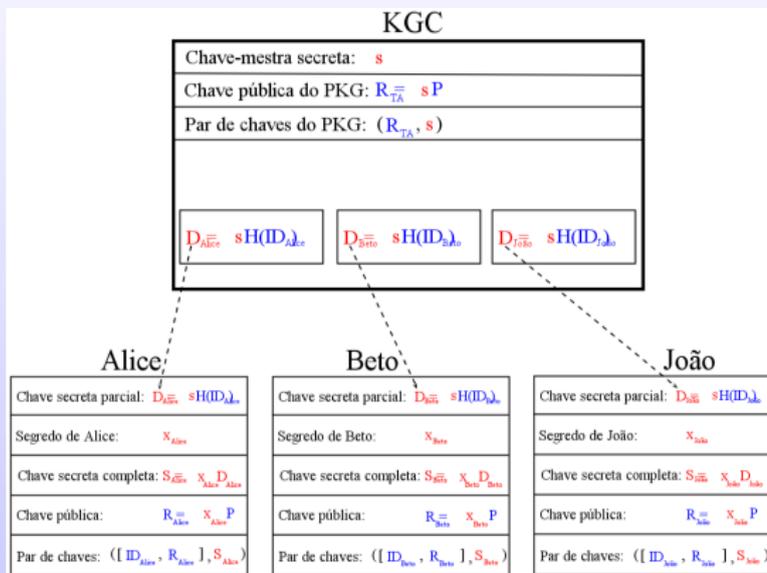


Figura: Distribuição das chaves privadas parciais no modelo sem certificado



IME - Instituto de
Matemática e Estatística

Android

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Sistema operacional baseado no núcleo *Linux*, para dispositivos móveis.
- Desenvolvido pelo *Google* e pela *Open Handset Alliance*.
- São disponibilizados dois kits de desenvolvimento para *Android*: **SDK** e **NDK**.



IME - Instituto de
Matemática e Estatística

Kits de Desenvolvimento

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- *Software Development Kit* (SDK): fornece bibliotecas de API e ferramentas de desenvolvimento necessárias para construir, testar e debugar aplicativos para *Android*. Possibilita a construção de aplicativos em linguagem Java.
- *Native Development Kit* (NDK): permite construir aplicativos ou parte de aplicativos utilizando linguagens de código nativo, como C e C++.
 - Nem sempre é vantajoso escrever parte de um aplicativo em código nativo.

Android SDK



IME - Instituto de Matemática e Estatística

Seminário de Segurança de Dados e Criptografia

Rafael Will M. de Araujo

Objetivos

Introdução

Desenvolvendo para Android

Proposta

Resultados Parciais

Opens the Android SDK Manager

Android SDK Manager

SDK Path: /home/rafael/android_development/android-sdk-linux/

Name	API	Rev.	Status
Tools			
Android 4.0.3 (API 15)			
API 13			
API 11			
API 10			
API 8			
Android 2.1 (API 7)			
SDK Platform	7	3	Installed
Samples for SDK	7	1	Installed
Extras			

Show: Updates/New Installed Obsolete Select [New or Updates](#)

Sort by: API level Repository [Deselect All](#)

Done loading packages.

Figura: Android Software Development Kit Manager

Android AVD



IME - Instituto de Matemática e Estatística

Seminário de Segurança de Dados e Criptografia

Rafael Will M. de Araujo

Objetivos

Introdução

Desenvolvendo para Android

Proposta

Resultados Parciais

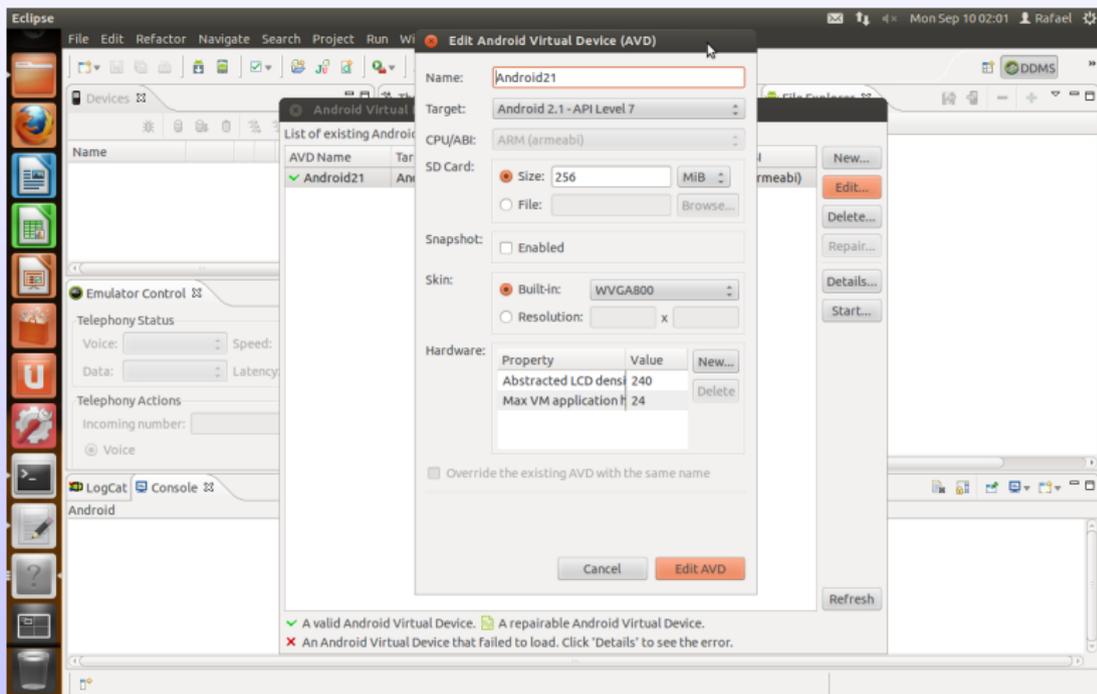


Figura: Android Virtual Device Manager

Android Emulator



IME - Instituto de Matemática e Estatística

Seminário de Segurança de Dados e Criptografia

Rafael Will M. de Araujo

Objetivos

Introdução

Desenvolvendo para Android

Proposta

Resultados Parciais

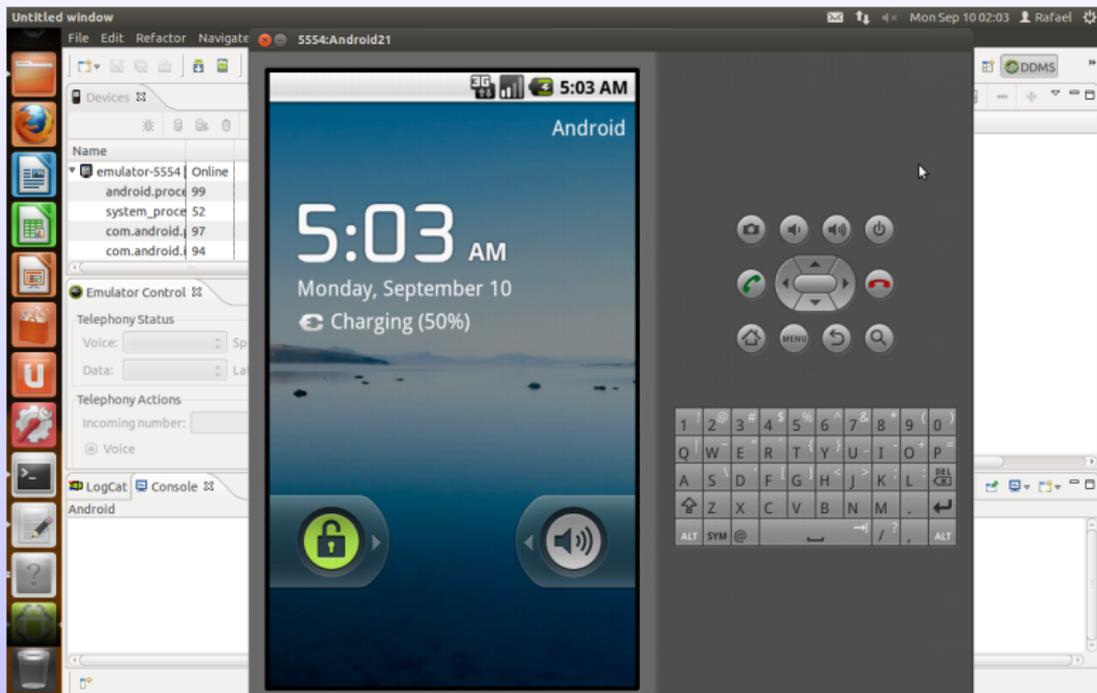


Figura: Emulador de *smartphone*

Android Emulator



IME - Instituto de Matemática e Estatística

Seminário de Segurança de Dados e Criptografia

Rafael Will M. de Araujo

Objetivos

Introdução

Desenvolvendo para Android

Proposta

Resultados Parciais

DDMS - Eclipse SDK

File Edit Refactor Navigate Search Project Run Window Help

Devices

Name	State	Android Z
emulator-5554	Online	Android21 [Z]
android.proce	99	8600
system_proce	52	8601
com.android.i	97	8602
com.android.i	94	8603

Emulator Control

Telephony Status

Voice: home Speed: Full

Data: home Latency: None

Telephony Actions

Incoming number:

Voice

LogCat Console

Android

File Explorer

Name	Size	Date	Time	Permissions	Info
app-private		2012-06-02	11:58	drwxrwx-x	
backup		2012-06-02	11:59	drwx---	
dalvik-cache		2012-06-06	05:11	drwxrwx-x	
data		2012-06-02	11:59	drwxrwx-x	
dontpanic		2012-06-02	11:58	drwxr-x--	
local		2012-06-08	04:00	drwxrwx-x	
tmp		2012-09-10	05:05	drwxrwx-x	
df-api9-e	638370	2012-06-08	04:00	-rwxrwxrwx	
df-api9-g	727317	2012-06-08	04:03	-rwxrwxrwx	
got01	336593	2012-06-18	07:24	-rwxrwxrwx	
test	4432	2012-09-10	05:05	-rwxrwxrwx	
lost-found		2012-06-02	11:58	drwxrwx--	
misc		2012-06-02	11:58	drwxrwx-t	
property		2012-06-06	05:11	drwx---	
system		2012-09-10	05:03	drwxrwx-x	
sdcard		1970-01-01	00:00	d-rwxr-x	

Figura: File Explorer

Android Terminal Emulator



IME - Instituto de
Matemática e Estatística

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

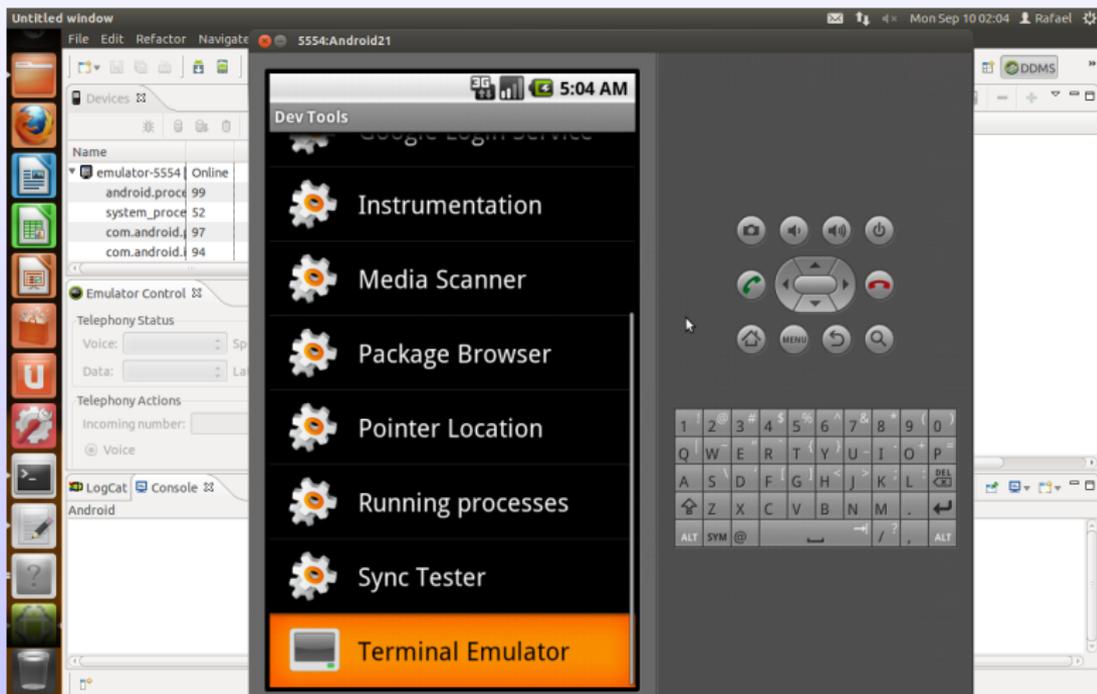


Figura: Android Virtual Device Manager

Android Terminal Emulator



IME - Instituto de Matemática e Estatística

Seminário de Segurança de Dados e Criptografia

Rafael Will M. de Araujo

Objetivos

Introdução

Desenvolvendo para Android

Proposta

Resultados Parciais

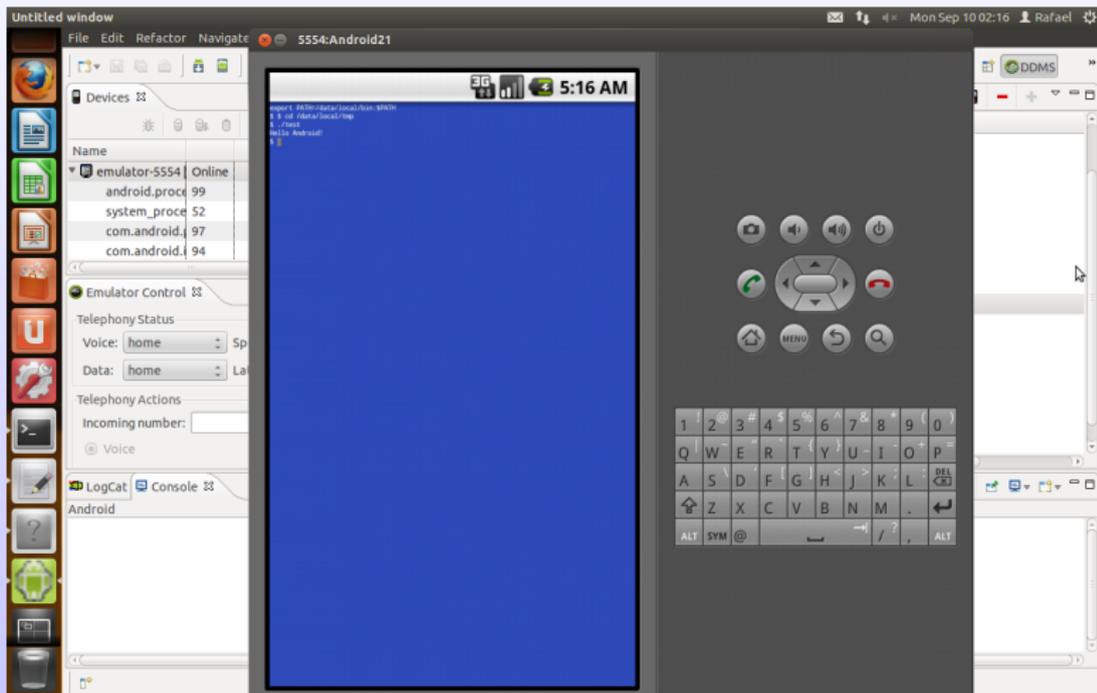


Figura: Android Virtual Device Manager

ADB - *Android Debug Bridge*



IME - Instituto de
Matemática e Estatística

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Localizado no diretório: `<sdk>/platform-tools/`

```
rafael@cripto: ~/android_development/android-sdk-linux/platform-tools
rafael@cripto:~/Desktop/meus_prot...  rafael@cripto:~/Desktop/meus_prot...  rafael@cripto:~/relic_toolkit/relic03...  rafael@cripto:~/android_develope...
rafael@cripto:~/android_development/android-sdk-linux/platform-tools$ ./adb shell
# cd /data/local/tmp
# chmod 777 test
# ./test
Hello Android:
#
```

Figura: *Android Debug Bridge*



IME - Instituto de
Matemática e Estatística

Relic-toolkit

Seminário de Segurança de Dados e Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais



- “RELIC is a modern cryptographic meta-toolkit with emphasis on efficiency and flexibility. RELIC can be used to build efficient and usable cryptographic toolkits tailored for specific security levels and algorithmic choices.”
- Disponível em: <http://code.google.com/p/relic-toolkit/>



IME - Instituto de
Matemática e Estatística

Relic-toolkit

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

RELIC: Modules

file:///C:/Documents%20and%20Settings/Rafael/Desktop/relic_c

RELIC 0.3.1

Main Page **Modules** Data Structures Files

Modules

Here is a list of all modules:

- Automated benchmarks.
- Multiple precision integer arithmetic.
- Core functions.
- Cryptographic protocols.
- Temporary double precision digit vector handling.
- Elliptic curves over binary fields.
- Elliptic curve cryptography.
- Prime elliptic curves.
- Binary field arithmetic.
- Prime field arithmetic.
- Ternary field arithmetic.
- Hyperelliptic genus 2 curves over binary fields.
- Hash functions.
- Pairings over binary elliptic curves.
- Pairing-based cryptography.
- Pairings over prime elliptic curves.
- Pseudo-random number generator.
- Automated tests.
- Misc utilities.

Generated on Fri Aug 10 2012 22:39:08 for RELIC by [doxygen](#) 1.7.6.1

Figura: Documentação da *Relic-toolkit*



IME - Instituto de
Matemática e Estatística

Relic-toolkit

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

```
RELIC: include/relic_pc.h file x
file:///C:/Documents%20and%20Settings/Rafael/Desktop/relic_c

#define g2_print(P) CAT(G2_LOWER, print)(P)
#define gt_print(P) CAT(GT_LOWER, print)(P)
#define g1_neg(R, P) CAT(G1_LOWER, neg)(R, P)
#define g2_neg(R, P) CAT(G2_LOWER, neg)(R, P)
#define gt_inv(R, P) CAT(GT_LOWER, inv)(R, P)
#define g1_add(R, P, Q) CAT(G1_LOWER, add)(R, P, Q)
#define g2_add(R, P, Q) CAT(G2_LOWER, add)(R, P, Q)
#define gt_mul(R, P, Q) CAT(GT_LOWER, mul)(R, P, Q)
#define g1_sub(R, P, Q) CAT(G1_LOWER, sub)(R, P, Q)
#define g2_sub(R, P, Q) CAT(G2_LOWER, sub)(R, P, Q)
#define g1_dbl(R, P) CAT(G1_LOWER, dbl)(R, P)
#define g2_dbl(R, P) CAT(G2_LOWER, dbl)(R, P)
#define gt_sqr(R, P) CAT(GT_LOWER, sqr)(R, P)
#define g1_norm(R, P) CAT(G1_LOWER, norm)(R, P)
#define g2_norm(R, P) CAT(G2_LOWER, norm)(R, P)
#define g1_mul(R, P, K) CAT(G1_LOWER, mul)(R, P, K)
#define g2_mul(R, P, K) CAT(G2_LOWER, mul)(R, P, K)
#define gt_exp(R, P, K) CAT(GT_LOWER, exp)(R, P, K)
#define g1_mul_gen(R, K) CAT(G1_LOWER, mul_gen)(R, K)
#define g2_mul_gen(R, K) CAT(G2_LOWER, mul_gen)(R, K)
#define g1_mul_pre(T, P) CAT(G1_LOWER, mul_pre)(T, P)
#define g2_mul_pre(T, P) CAT(G2_LOWER, mul_pre)(T, P)
#define g1_mul_fix(R, T, K) CAT(G1_LOWER, mul_fix)(R, T, K)
#define g2_mul_fix(R, T, K) CAT(G2_LOWER, mul_fix)(R, T, K)
#define g1_mul_sim(R, P, K, Q, L) CAT(G1_LOWER, mul_sim)(R, P, K, Q, L)
#define g2_mul_sim(R, P, K, Q, L) CAT(G2_LOWER, mul_sim)(R, P, K, Q, L)
#define g1_mul_sim_gen(R, K, Q, L) CAT(G1_LOWER, mul_sim_gen)(R, K, Q, L)
#define g2_mul_sim_gen(R, K, Q, L) CAT(G2_LOWER, mul_sim_gen)(R, K, Q, L)
#define g1_map(P, M, L) ; CAT(G1_LOWER, map)(P, M, L)
#define g2_map(P, M, L) ; CAT(G2_LOWER, map)(P, M, L)
#define pc_map(R, P, Q) ; CAT(PC_LOWER, map)(R, P, Q)
```

Figura: Documentação da *Relic-toolkit*



IME - Instituto de
Matemática e Estatística

Relic-toolkit

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

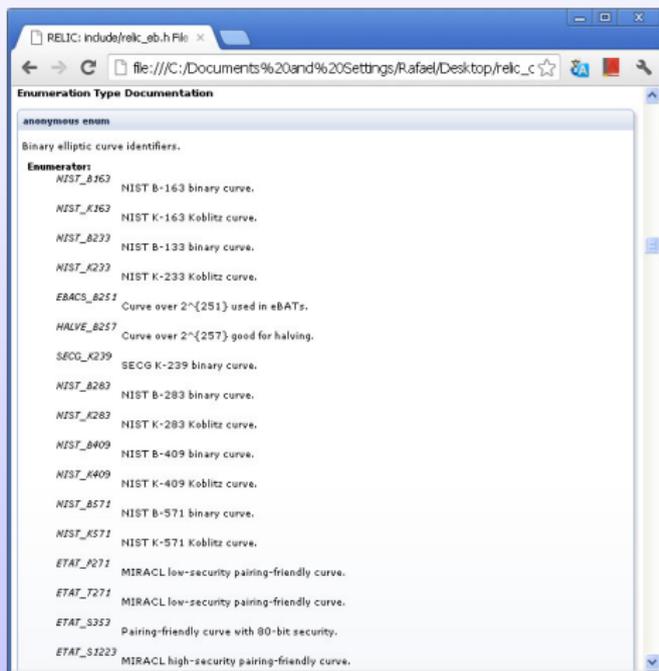


Figura: Curvas elípticas disponíveis para corpos binários



IME - Instituto de
Matemática e Estatística

Relic-toolkit

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

```
rafael@crypto: ~/relic_toolkit/relic031-x86
Page 1 of 3
ALIGN          1
ALLOC          AUTO
ARCH           X86
ARITH          easy
BENCH         1
BITGED        OFF
BN_KARAT       0
BN_MAGNI      DOUBLE
BN_METHOD     COMBA;COMBA;MONTY;SLIDE;BASIC;BASIC
BN_PRECI      400
CHECK         ON
CMAKE_BUILD_TYPE
CMAKE_INSTALL_PREFIX /usr/local
COLOR         ON
COMP          1
CORES         1
CP_METHOD     QUICK
CP_RSAPD      PKCS1
DEBUG         OFF
DOCUM         ON
EB_DEPTH      4
EB_KBLTZ      ON
EB_METHOD     PROJ3;LWNAF;COMBS;INTER
EB_MIXED      ON
EB_ORDIN      ON
EB_PRECO      ON
EB_SUPER      ON
EB_WIDTH      4
EC_KBLTZ      ON
EC_METHOD     BINAR
EP_DEPTH      4
EP_KBLTZ      ON
EP_METHOD     PROJ3;LWNAF;COMBS;INTER
EP_MIXED      ON

ALIGN: Boundary to align digit vectors
Press [enter] to edit option
Press [c] to configure
Press [h] for help          Press [q] to quit without generating
Press [t] to toggle advanced mode (Currently Off)

CMake Verston 2.8.7
```

Figura: Algumas opções de compilação da *Relic-toolkit*



IME - Instituto de
Matemática e Estatística

Android NDK Toolchains

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

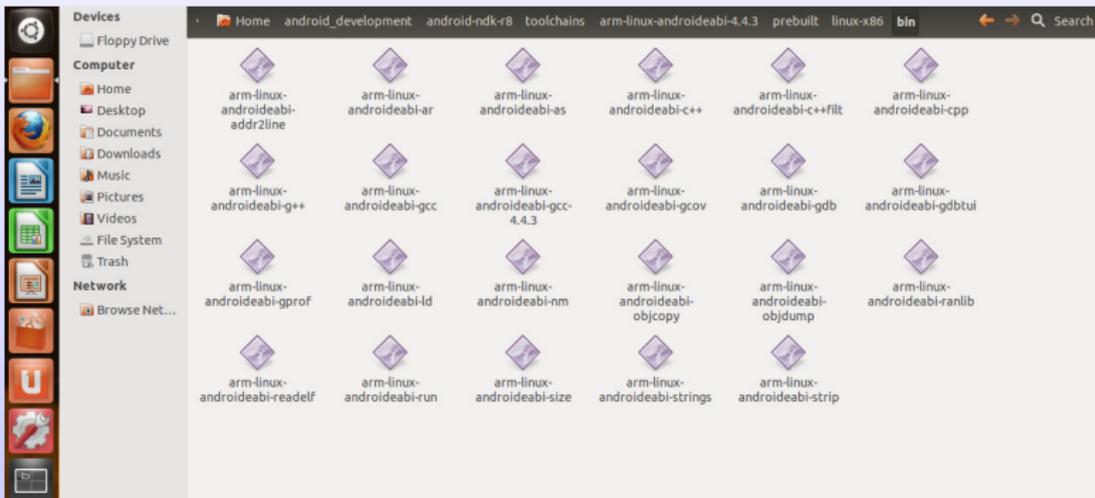
Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais





IME - Instituto de
Matemática e Estatística

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

Variáveis de ambiente

```
android_env.sh ✖
1 #!/bin/sh
2 export NDK=$HOME/android_development/android-ndk-r8
3 SYSROOT=$NDK/platforms/android-9/arch-arm
4
5 MIDDLE=toolchains/arm-linux-androideabi-4.4.3/prebuilt/linux-x86/bin
6 PREF=arm-linux-androideabi-
7
8 export CC="$NDK/$MIDDLE/${PREF}gcc --sysroot=$SYSROOT"
9 export CXX="$NDK/$MIDDLE/${PREF}g++ --sysroot=$SYSROOT"
10 export LD="$NDK/$MIDDLE/${PREF}ld --sysroot=$SYSROOT"
11 export CPP="$NDK/$MIDDLE/${PREF}cpp --sysroot=$SYSROOT"
12 export AS="$NDK/$MIDDLE/${PREF}as --sysroot=$SYSROOT"
13 export OBJCOPY="$NDK/$MIDDLE/${PREF}objcopy --sysroot=$SYSROOT"
14 export OBJDUMP="$NDK/$MIDDLE/${PREF}objdump --sysroot=$SYSROOT"
15 export STRIP="$NDK/$MIDDLE/${PREF}strip --sysroot=$SYSROOT"
16 export RANLIB="$NDK/$MIDDLE/${PREF}ranlib --sysroot=$SYSROOT"
17 export CCLD="$NDK/$MIDDLE/${PREF}gcc --sysroot=$SYSROOT"
18 export AR="$NDK/$MIDDLE/${PREF}ar --sysroot=$SYSROOT"
```

Figura: Configurando algumas variáveis de ambiente para facilitar o processo de compilação



IME - Instituto de
Matemática e Estatística

Ponto de Partida

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Projeto Borboleta (Fapesp).
 - Um dispositivo móvel (PDA) deseja se comunicar com um servidor de banco de dados de forma segura.
- Comparar o cenário existente no projeto Borboleta caso fossem utilizados outros protocolos de acordo de chave.
- Utilização da biblioteca **Relic Toolkit**, em linguagem C.
 - Suporte para curvas elípticas.
 - Suporte para emparelhamentos bilineares.
 - Crescente uso pela comunidade acadêmica.
 - Documentação via *doxygen*, e frequente correção de *bugs*.



Cenário

IME - Instituto de
Matemática e Estatística

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

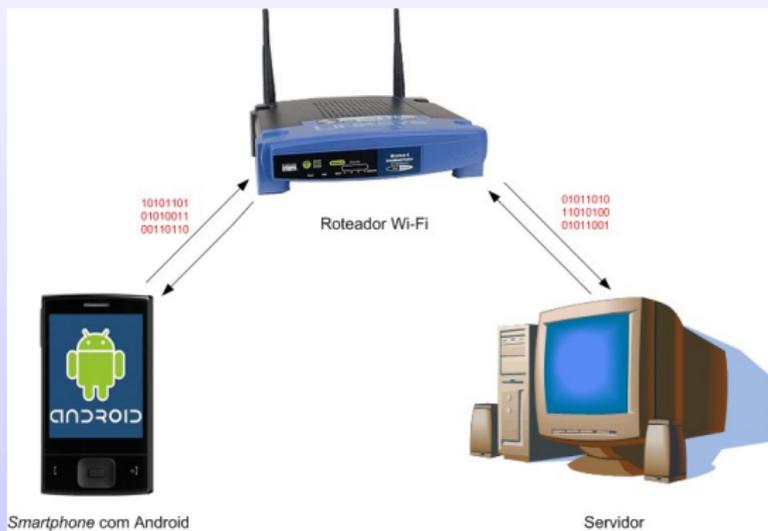


Figura: Cenário a ser estudado



IME - Instituto de
Matemática e Estatística

Comunicação Servidor-Smartphone

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Escolhemos utilizar *sockets* em linguagem C.
 - Comunicação TCP/IP.
 - Integra-se facilmente aos outros códigos construídos (todo o código fica escrito em linguagem C).
 - Redução de *overhead*. Protocolos de comunicação mais complexos carregam outros “dados extras”.
 - Ausência de funções na *Relic-toolkit* para transformação de certos tipos em *strings*.



IME - Instituto de
Matemática e Estatística

Seminário de Segurança de Dados e Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

Protocolos implementados

- Até o momento, implementamos 3 protocolos do modelo sem certificado:
 - LBG (BDH e Gap-BDH).
 - GOT (BDH e Gap-BDH).
 - GNT (Gap-BDH).
- Curvas utilizadas:
 - ETAT_T271 (segurança de 64 bits).
 - ETAT_S353 (segurança de 80 bits).
 - ETAT_S1223 (segurança de 128 bits).
- Versão da *Relic-toolkit*: 0.3.1



IME - Instituto de
Matemática e Estatística

Equipamento utilizado

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Servidor:
 - Modelo: Compaq CQ-50 113BR.
 - Processador: Intel Core 2 Duo T5800, 2.0 GHz.
 - Memória RAM: 3GB DDR2, 800 MHz.
 - Conexão de rede: por cabo, 100 Mbps.
 - Sistema operacional: Ubuntu 10.04 LTS, 64 bits.
- *Smartphone*:
 - Modelo: Motorola Milestone.
 - Processador: ARM Cortex-A8, 600 MHz.
 - Memória RAM: 256 MB.
 - Conexão de rede: Wi-Fi (802.11g), 54 Mbps.
 - Sistema operacional: Android 2.2



IME - Instituto de
Matemática e Estatística

Equipamento utilizado

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

- Roteador Wi-Fi:
 - Modelo: D-Link DIR-300.
 - Processador: Atheros AR2317, 183 MHz.
 - Memória RAM: 16 MB.
 - Conexão de rede: 4x 100 Mbps (cabo), e Wi-Fi de 54 Mbps.
 - Sistema operacional: DD-WRT v24.



IME - Instituto de
Matemática e Estatística

Resultados (curva ETAT_T271)

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

	GNT (Gap-BDH)	GOT (Gap-BDH)	LBG (Gap-BDH)	GOT (BDH)	LGB (BDH)
Tempo total (10 rodadas) sem pré-computação	0,882	0,904	1,072	1,383	1,725
Tempo médio de uma única sessão	0,088	0,090	0,107	0,138	0,172
Tempo total (10 rodadas) com pré-computação	0,587	0,466	0,634	0,559	0,906
Tempo médio de uma única sessão	0,059	0,047	0,063	0,056	0,091
Memória utilizada pelas variáveis do programa (bytes)	2700	2364	2364	3132	3132
Tráfego na rede por sessão (bytes)	448	448	448	448	448

(Tempo em segundos)



IME - Instituto de
Matemática e Estatística

Resultados (curva ETAT_T353)

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

	GNT (Gap-BDH)	GOT (Gap-BDH)	LBG (Gap-BDH)	GOT (BDH)	LGB (BDH)
Tempo total (10 rodadas) sem pré-computação	1,556	1,664	1,953	2,617	3,339
Tempo médio de uma única sessão	0,156	0,166	0,195	0,262	0,334
Tempo total (10 rodadas) com pré-computação	0,987	0,815	1,104	1,019	1,728
Tempo médio de uma única sessão	0,099	0,082	0,110	0,102	0,173
Memória utilizada pelas variáveis do programa (bytes)	3552	3108	3108	4128	4128
Tráfego na rede por sessão (bytes)	592	592	592	592	592

(Tempo em segundos)



IME - Instituto de
Matemática e Estatística

Resultados (curva ETAT_T1223)

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

	GNT (Gap-BDH)	GOT (Gap-BDH)	LBG (Gap-BDH)	GOT (BDH)	LGB (BDH)
Tempo total (10 rodadas) sem pré-computação	32,169	34,852	41,833	56,134	72,629
Tempo médio de uma única sessão	3,217	3,485	4,183	5,613	7,263
Tempo total (10 rodadas) com pré-computação	19,642	15,503	22,368	19,554	35,885
Tempo médio de uma única sessão	1,964	1,550	2,237	1,955	3,588
Memória utilizada pelas variáveis do programa (bytes)	11244	9828	9828	13116	13116
Tráfego na rede por sessão (bytes)	1888	1888	1888	1888	1888

(Tempo em segundos)



IME - Instituto de
Matemática e Estatística

Comparação entre os protocolos (tempos sem pré-computação)

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

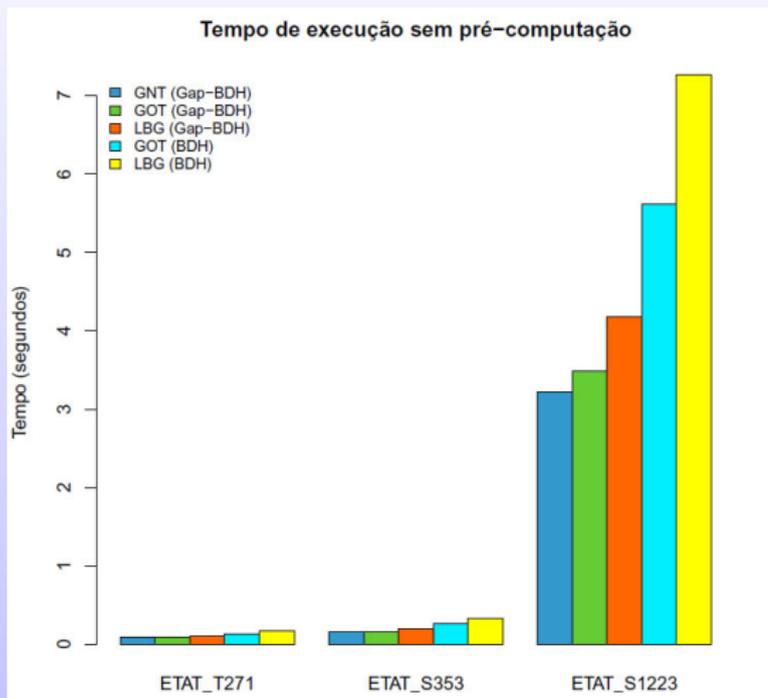
Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais





IME - Instituto de
Matemática e Estatística

Comparação entre os protocolos (tempos com pré-computação)

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

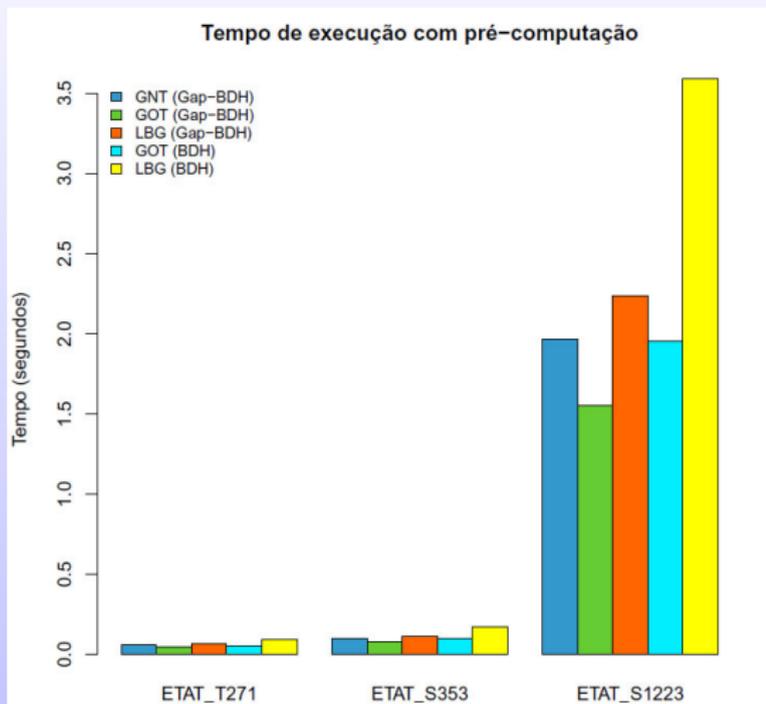
Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais





IME - Instituto de
Matemática e Estatística

Comparação entre os protocolos (consumo de memória)

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

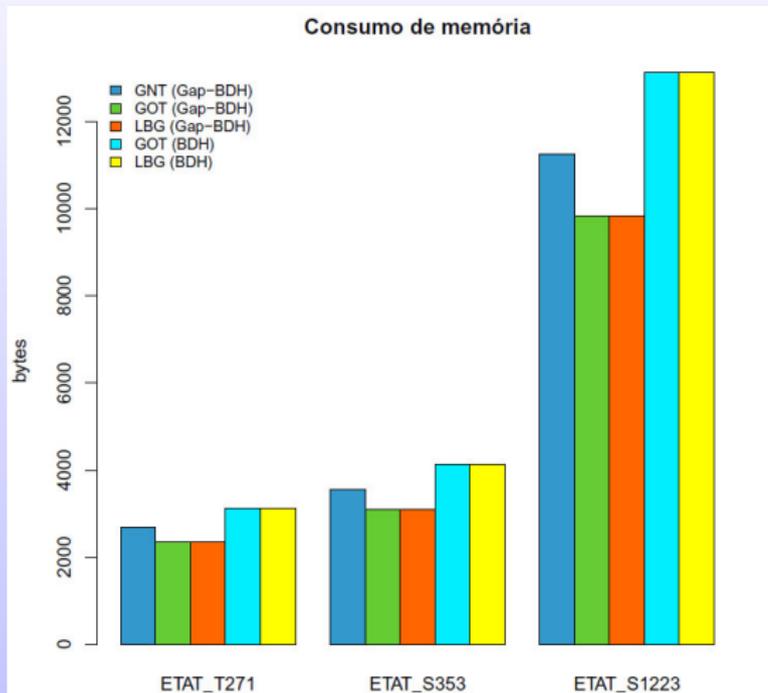
Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais





IME - Instituto de
Matemática e Estatística

Próximos passos

Seminário de Segurança de Dados e Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

**Resultados
Parciais**

- Elaboração do relatório do CNPq.
- Escolha de novos protocolos para implementação.



IME - Instituto de
Matemática e Estatística

Perguntas?

Seminário de
Segurança de
Dados e
Criptografia

Rafael Will
M. de Araujo

Objetivos

Introdução

Desenvolvendo
para Android

Proposta

Resultados
Parciais

