تام: تلفن امن من

TAM MTD : Mobile Threat Defense

موضوعات

چه مشکلاتی توسط تام حل میگردد؟

قابلیت های تام

اهداف

تام چیست؟

چرا به تام نیاز داریم؟

UEM چیست؟

اطلاعات سازمانی،
لیست مشتریان،
اطلاعات تماس...

ایمیل

موقعیت لحظه به
لحظه، فعالیت
ها...

سلامت

جزئیات جلسات،
محل قرار ملاقات
ها...

تقویم

شماره های تماس،
نام و آدرس
مخاطبان...

مخاطبان

تهدید های لایهٔ سیستم

آسیب پذیری های
سیستم عامل،
تنظیمات نا امن...

تهدید های لایهٔ شبکه

حملات فیشینگ،
سرقت اطلاعاتِ
نشست، MITM...

تهدید های لایهٔ اَپلیکیشن

سرقت اطلاعات،
باج افزار، کنترل از
راه دور...

تلفن امن من (تام)

حفاظت از لایهٔ سیستم

شناسایی و گزارش تنظیمات مخاطره آمیز.

شرح: شناسایی و گزارش تنظیمات حساس اعمال شده بر روی دستگاه که منجر به وقوع آسیب پذیری و سوء استفاده های آتی میگردند.

مثال: در صورت فعال بودن دسترسی **ریشه** بدافزارها این امکان را خواهند داشت تا با برخورداری از سطح دسترسی کامل، دستگاه را کنترل نمایند.

مدیریت بروز رسانی های امنیتی.

شرح: شناسایی و گزارش نسخه های قدیمی سیستم عامل و اپلیکیشن های حساس سیستمی.

مثال: در صورت بروز نبودن نسخهٔ سیستم عامل، دستگاه کاربر در معرض آسیب پذیری های امنیتی قرار خواهد گرفت.

تلفن امن من (تام)

حفاظت از لایهٔ شبکه

حفاظت در مقابل حملات فیشینگ.

شرح: حفاظت در برابر حملات فیشنگ از طریق اعتبار سنجی و اصالت سنجی شناسهٔ منابع تحت شبکه و certificate ارائه شده.

مثال: در صورتیکه کاربر از یک URL مرتبط با فیشینگ بازدید نماید، قبل از پردازش درخواست و نشت اطلاعات حساس درخواست مسدود خواهد گردید.

حفاظت تحت شبکهٔ درون دستگاه (ONP)

شرح: حفاظت در برابر شبکه های مخرب، حملات مرد میانی و حملات فیشینگ از طریق اعتبار سنجی پارامتر های امنیتی شبکه.

مثال: در صورتیکه کاربر به یک شبکهٔ بی سیم با رمزنگاری ضعیف متصل گردد، شبکه مسدود خواهد گردید.

تلفن امن من (تام)

حفاظت از لایهٔ اپلیکیشن

تحلیل ایستا.

شرح: استخراج کد منبع (به همراه کتابخانه های شخص ثالث) و بررسی خطاهای امنیتی، خطاهای برنامه نویسی و خطاهای منجر به کاهش کارکرد.

مثال: اگر در کد منبع یک حلقهٔ بی نهایت یافت گردد، در راستای جلوگیری از کاهش کارکرد گزارش میگردد.

تحلیل پویا.

شرح: شناسایی بد افزار از طریق اجرای اپ بر روی سند باکس؛ اعمال تحلیل رفتاری، نظارت بر تعاملات مبتنی بر شبکه و نظارت بر تعاملات مبتنی بر فایل سیستم.

مثال: کلیهٔ درخواست هایی که اپلیکیشن به سمت وب سرویس ارسال مینماید، در مرحلهٔ تحلیل پویا مورد بررسی قرار خواهند گرفت.

تلفن امن من (تام)

حفاظت از لایهٔ اپلیکیشن

تحلیل مجوز.

شرح: شناسایی بد افزار از طریق بررسی مجوزات درخواستی با استفاده از هوش مصنوعی مبتنی بر شبکه های عصبی.

مثال: در صورتیکه لیست مجوزات درخواستی مشابه با لیست مجوزات بد افزار ها باشد، بر اساس الگوهای یادگیری ماشین اپلیکیشن به عنوان یک تهدید بالقوه شناسایی و گزارش میگردد.

شناسایی باج افزار.

شرح: نظارت مستمر بر روی فایل سیستم، شناسایی حمله و بازگشت به نقطهٔ امن.

مثال: در صورت مشاهدهٔ هرگونه تغییر مشکوک بر روی فایل ها، کپی برداری از فایل ها انجام گردیده، پروسهٔ مشکوک متوقف گردیده و تاریخچهٔ آن بررسی میگردد؛ فایل های اصلی باز گردانی شده و فایل های مشکوک حذف میگردد.

Anti Malware

تحلیل رفتاری اپلیکیشن ها

شناسایی مجوزات خطرناک

کشف آسیب پذیری اپلیکیشن ها

Anti Sniff

شناسایی آدرس های phishing

اعتبار سنجی certificate ها

ارزیابی رمزگذاری ها

Anti Theft

تعریف حصار جغرافیایی

قفل دستگاه از راه دور

پاکسازی دستگاه از راه دور

Anti Leak

قفل اَپ ها و سرویس ها

لیست سیاه تماس ها

شناسایی پیامک های مشکوک

ضد بد افزار

ارائه گزارش ریسک

اجرای اپ بر روی سند باکس

تحلیل تراکنش های I/O

ضد شنود

وب گردی امن

تحلیل تعاملات تحت شبکه

جلوگیری از حملات MITM

ضد سرقت

مدیریت از راه دور

هشدار صوتی در هنگام سرقت

ارسال لحظه به لحظهٔ مکان

ضد شنود

حفاظت از برنامه های سیستم

حفاظت از سرویس های شبکه

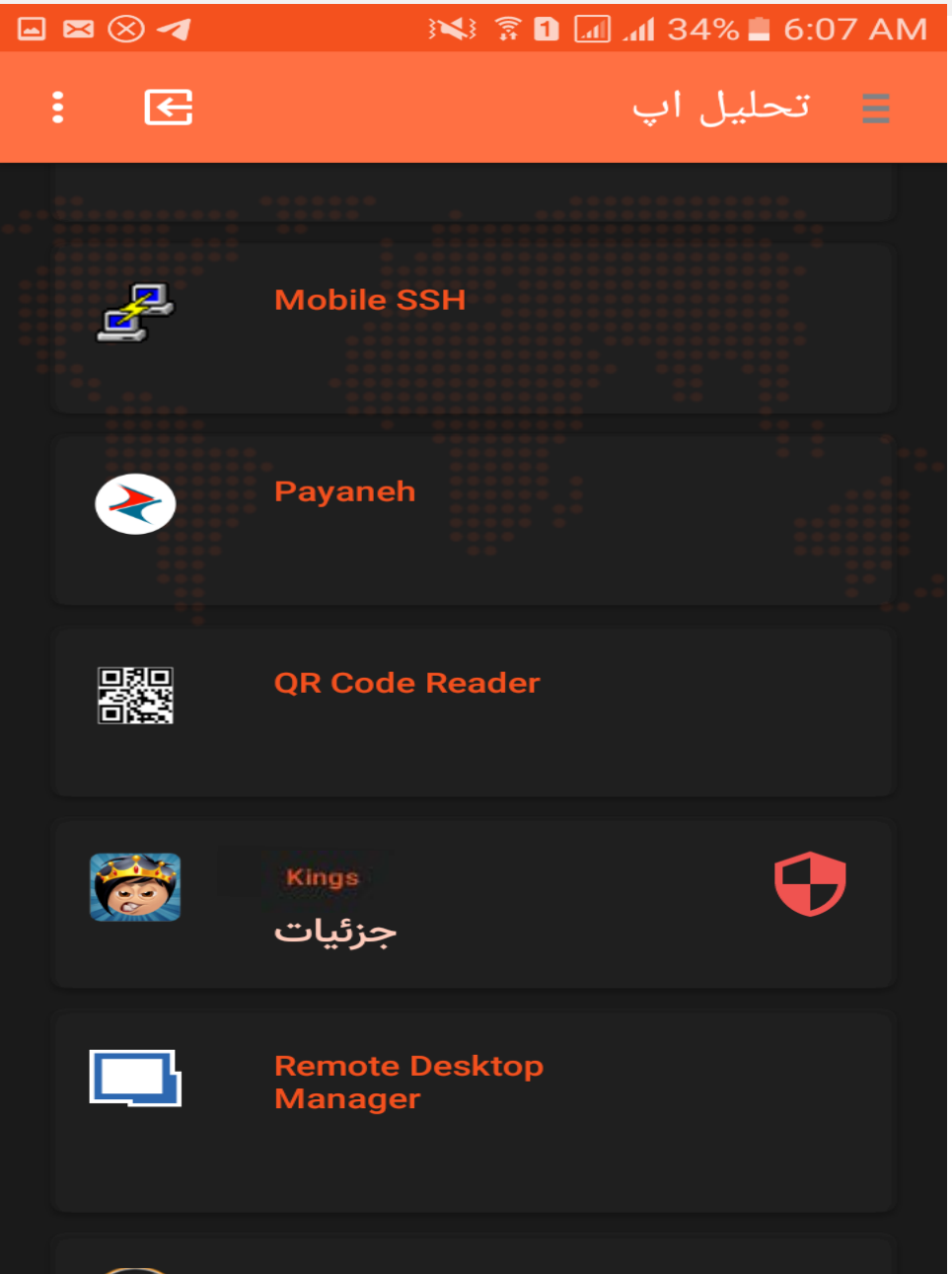
حفاظت از پیامک های مخرب

ارتباط گستر خاورمیانه

ضد بد افزار

تلفن امن من (تام)

تحلیل امنیتی اپلیکیشن ها



تحلیل امنیتی اَپ بصورت **استاتیک**:

- بررسی سورس کد اَپ
- کشف ناهنجاری های **بدافزاری**
- کشف **آسیب پذیری** های امنیتی
- کشف ناهنجاری های **رفتاری**
- تحلیل مجوزات خطرناک
- ارائه گزارش ریسک

تلفن امن من (تام)

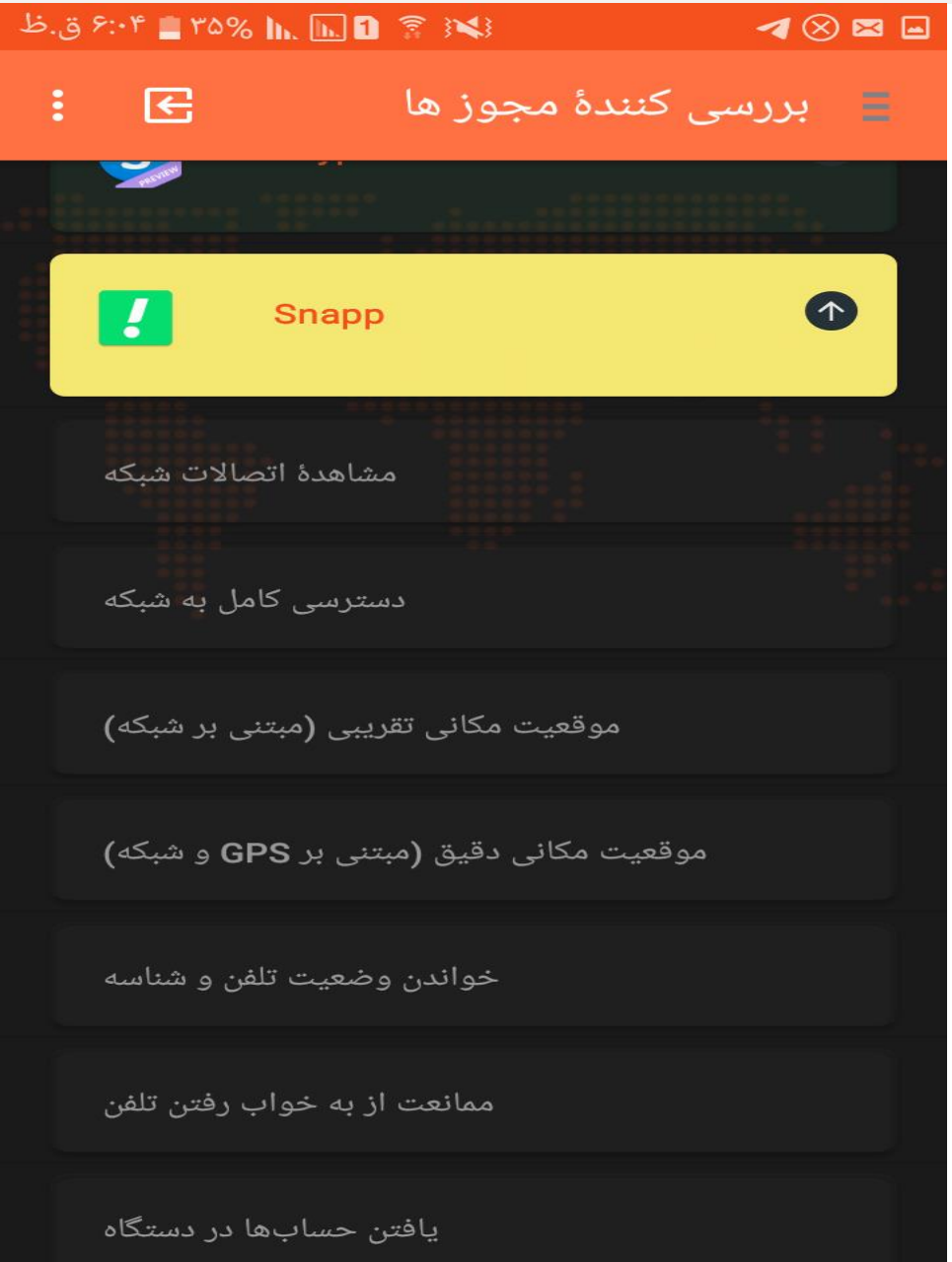
تحلیل امنیتی اپلیکیشن ها

تحلیل امنیتی اَپ بصورت **داینامیک**:

- اجرای اَپ بر روی **سند باکس**
- تحلیل **رفتاری** در زمان اجرا
- تحلیل تعاملات شبکه و اینترنت
- تحلیل تراکنش های مبتنی بر **پایگاه داده**
- تحلیل **ورودی / خروجی**

تلفن امن من (تام)

تحلیل امنیتی اپلیکیشن ها



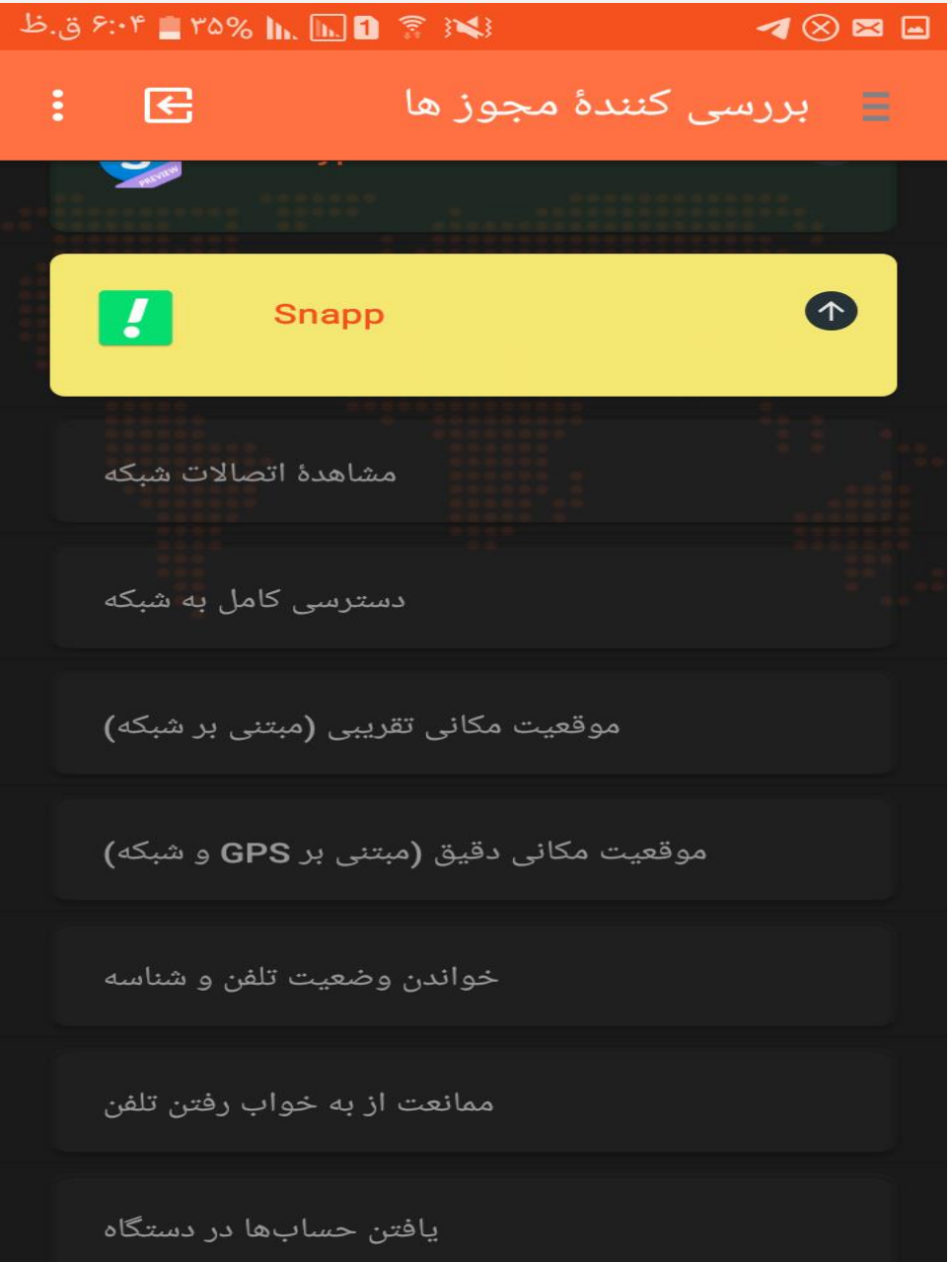
شناسایی مجوزات خطرناک هر اَپ

- تحلیل دامنهٔ امنیتی مبتنی بر PTD
- هوش مصنوعی بر پایه شبکه های عصبی
- تشخیص میزان تخریب
- ارائه مدل تهدید

تلفن امن من (تام)

مکانیزم ضد باج افزار

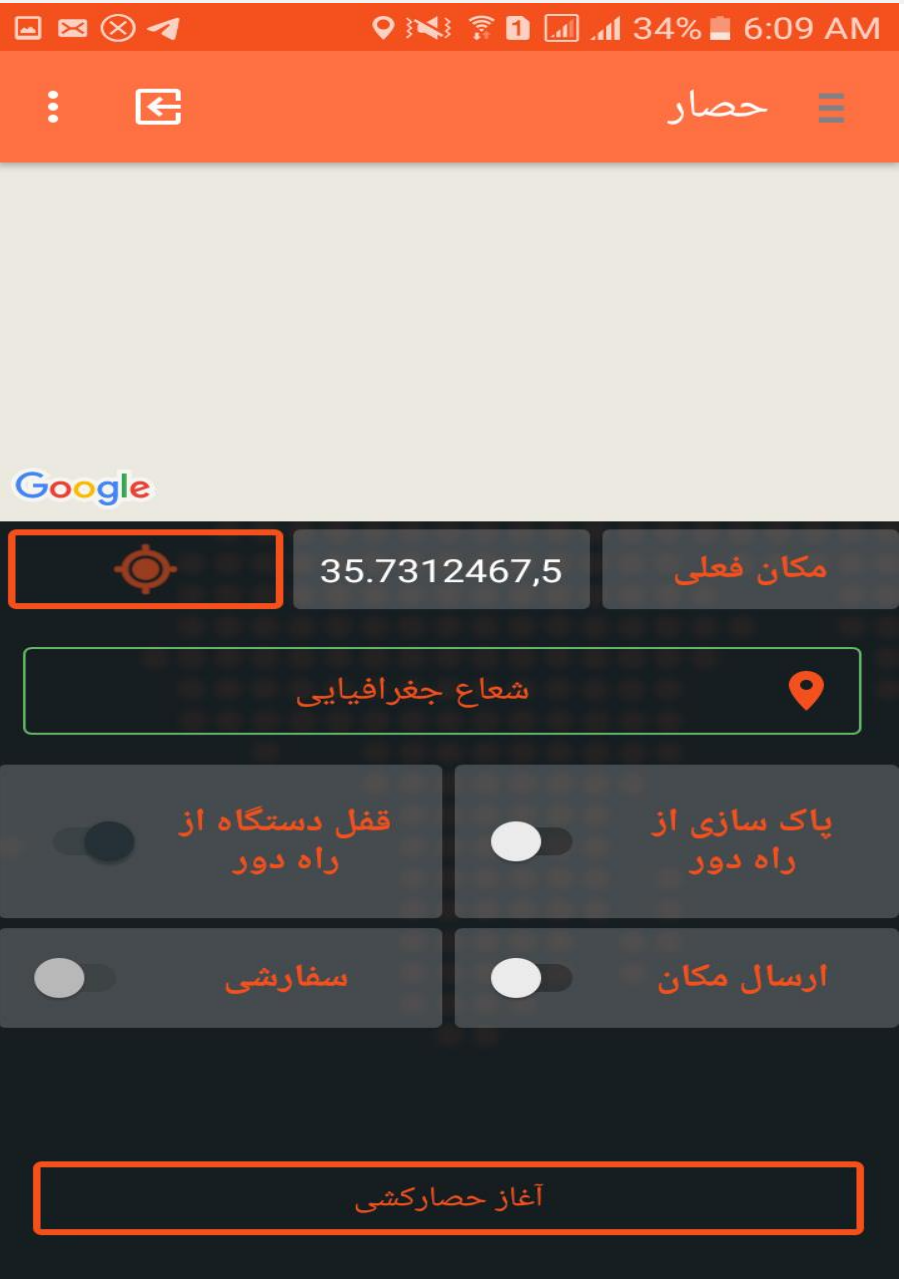
- نظارت بر فایل سیستم
- شناسایی باج افزار
- بازگشت به نقطهٔ امن
- گزارش



ضد سرقت

تلفن امن من (تام)

سیستم ضد سرقت



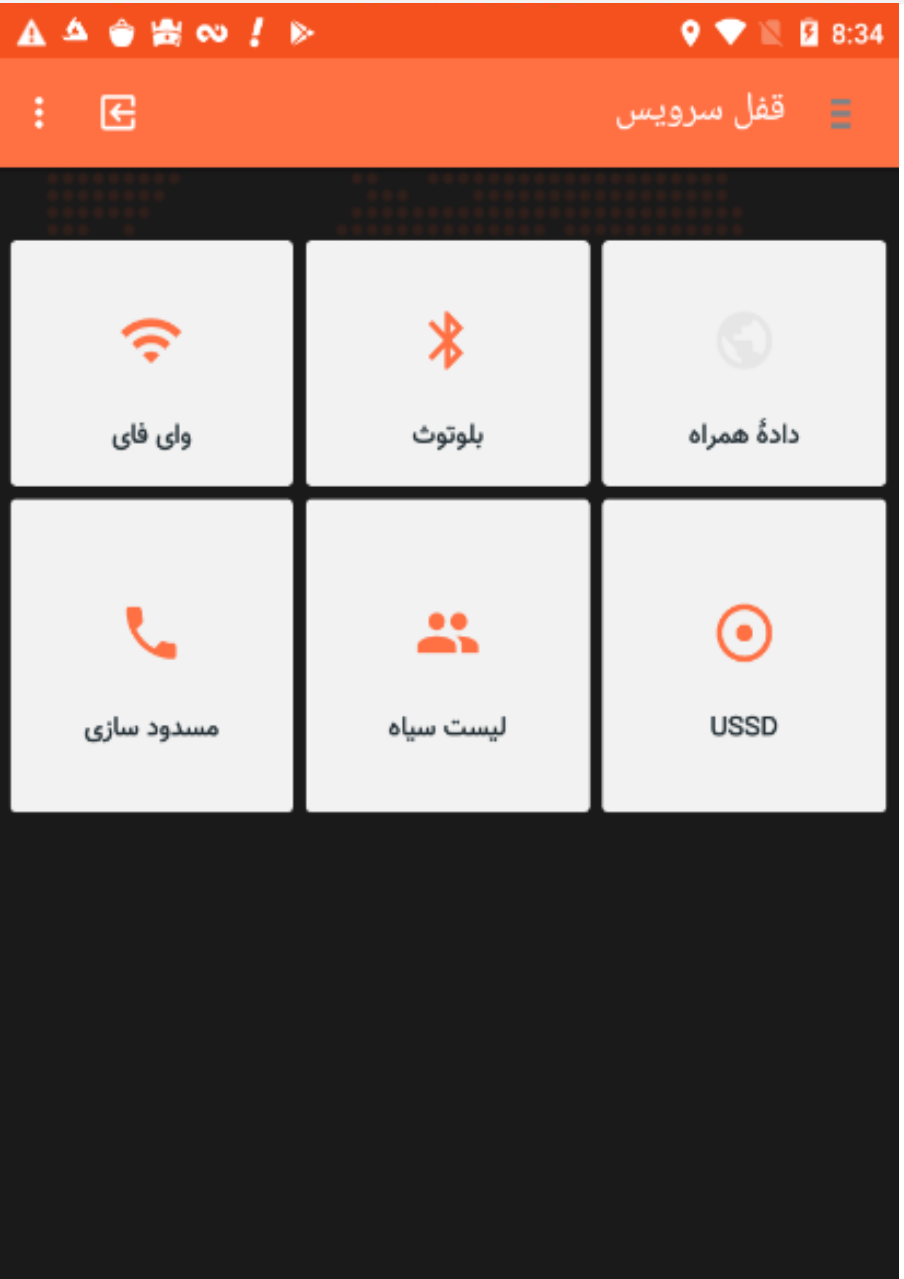
- ایجاد **حصار جغرافیایی** بر اساس **شعاع** تعریف شده
- ایجاد **هشدار صوتی** در صورت **خروج** از حصار جغرافیایی
- امکان **مدیریت از راه دور** با استفاده از تعریف **شمارهٔ نگاهبان:**
  - امکان **قفل دستگاه** بصورت از راه دور
  - امکان **پاکسازی دستگاه** بصورت از راه دور
  - امکان **ارسال مکان** لحظه به لحظهٔ دستگاه به شمارهٔ نگاهبان

ضد شنود

تلفن امن من (تام)

قفل سرویس ها

- قابلیت قفل سرویس های تحت شبکه
- قابلیت تعریف لیست سیاه تماس
- قابلیت تعریف لیست سیاه پیامک
- قابلیت تعریف لیست سیاه USSD



ارتباط گستر خاورمیانه

تماس با لیست سیاه

تماس های خروجی از لیست سیاه مسدود شود.

همین خوبه

مخاطبین من نیستند

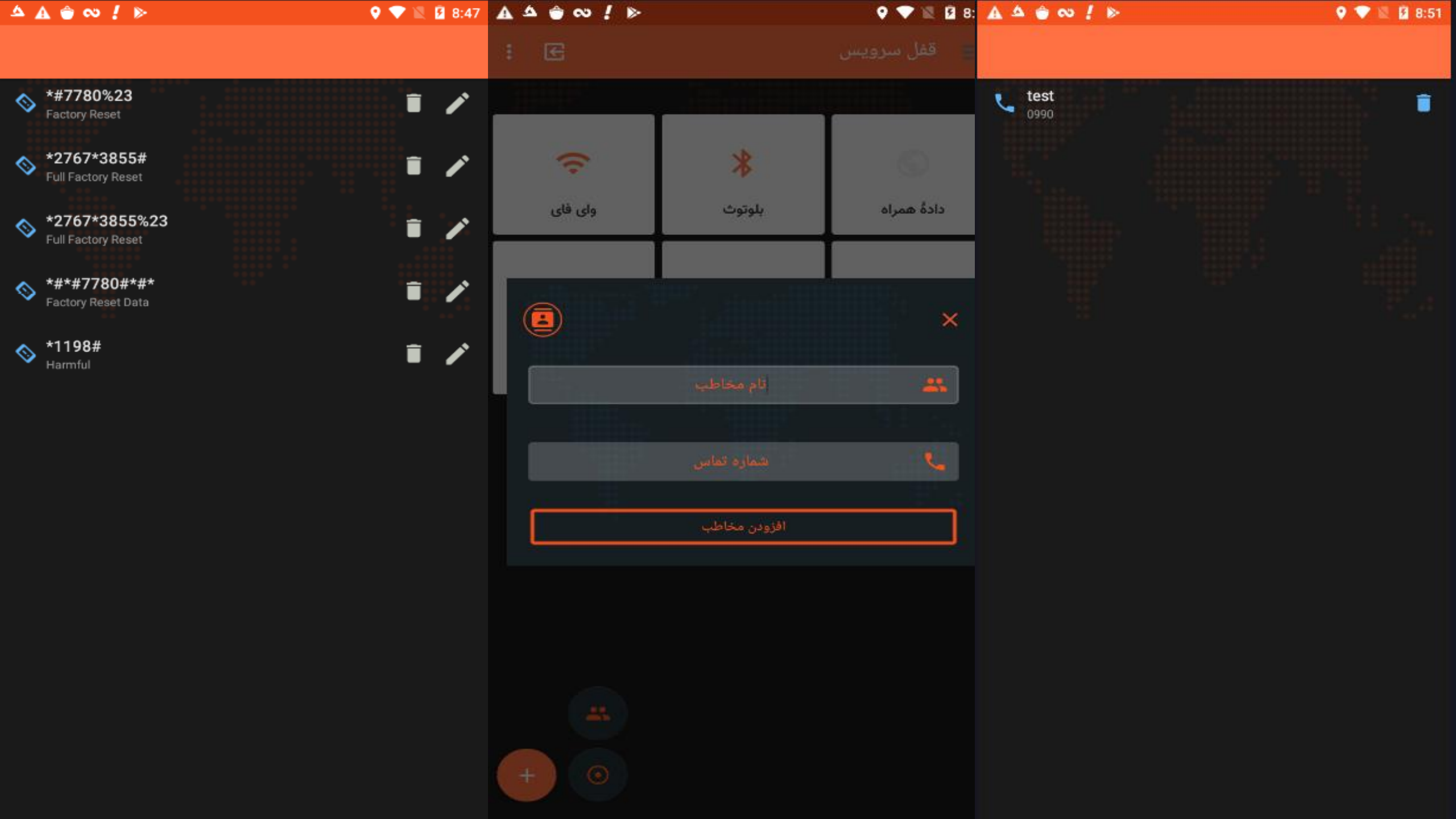
مسدود سازی تماس از شماره های ذخیره نشده

همین خوبه

اصلاً و ابداً

هیچ تماسی مسدود نشود.

همین خوبه


8:47
*#7780%23
Factory Reset
*2767*3855#
Full Factory Reset
*2767*3855%23
Full Factory Reset
##7780#*#*
Factory Reset Data
*1198#
Harmful
قفل سرویس
وای فای
بلوتوث
دادهٔ همراه
نام مخاطب
شماره تماس
افزودن مخاطب
8:51
test
0990

با سپاس