IRONFOX

BY INNOVERA TECHNOLOGY

Website, Mobile Apps & API Protection

Khalegh Salehi
Founder & Developer

INNOVERA TECH

Innovera Professional Service

- SECURITY AND SOFTWARE DEVELOPMENT
- PENETRATION TESTING
- CODE REVIEW
- APPLICATION AND SERVICE HARDENING

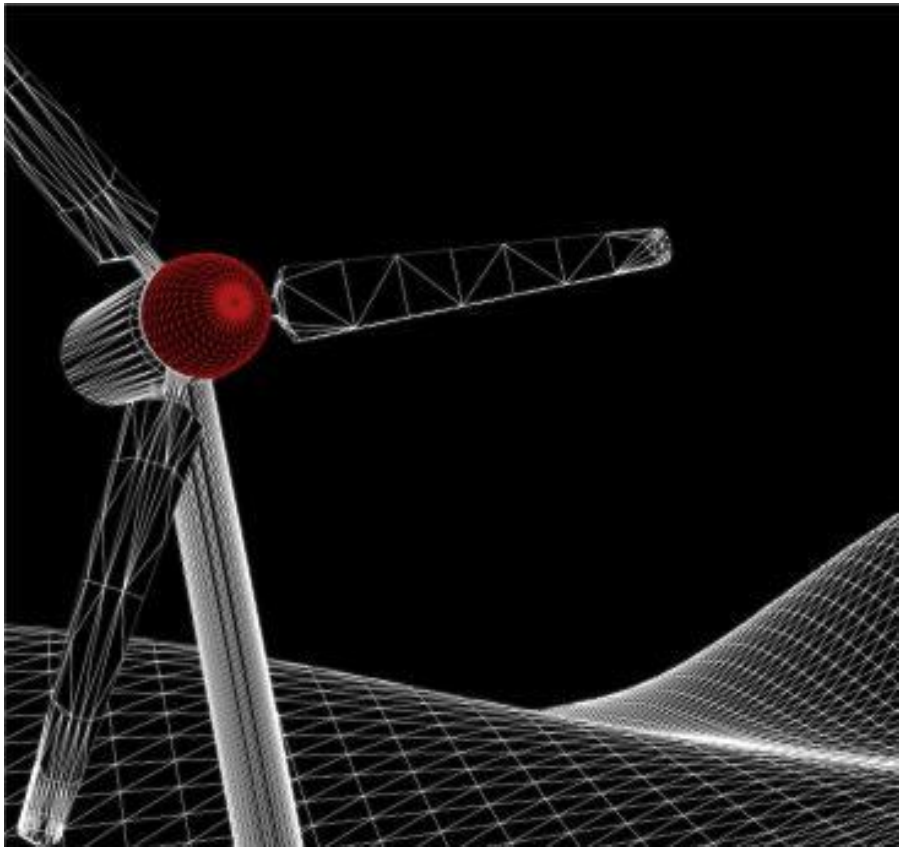


Image © IoActive

INNOVERA TECH

Innovera Security Solutions

- Web layer DoS/DDoS attacks protection
  - IronFox
- Fuzzing & fault injection
  - LuFuzz
- Mobile (iOS, Android) & API protection
  - AppArmor

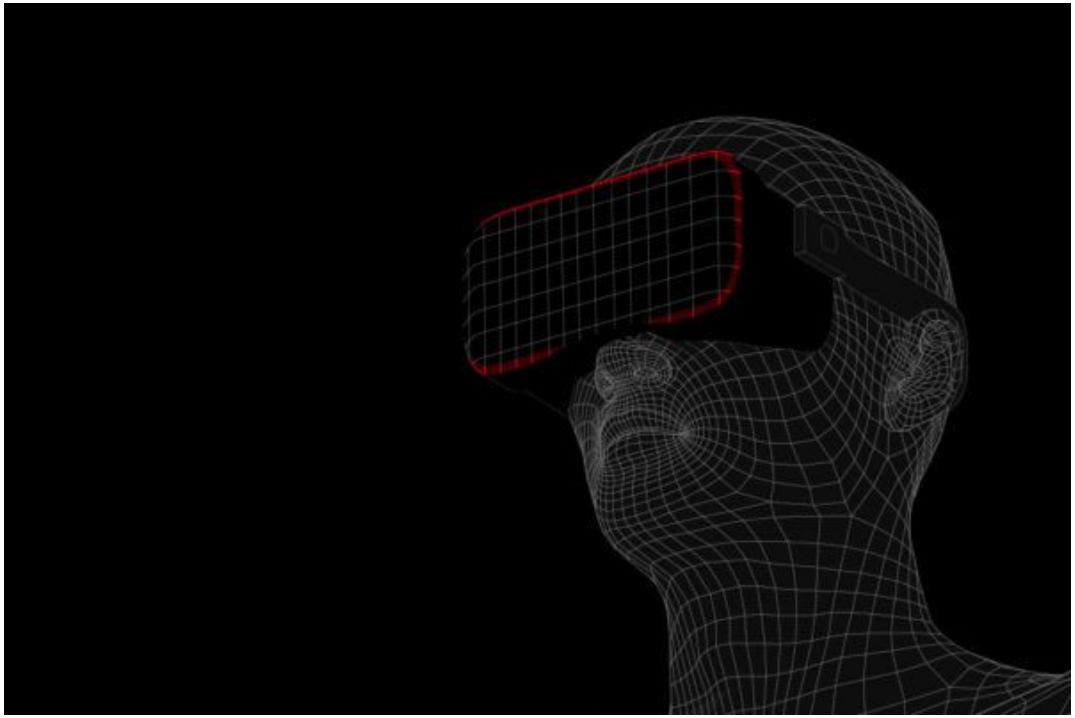
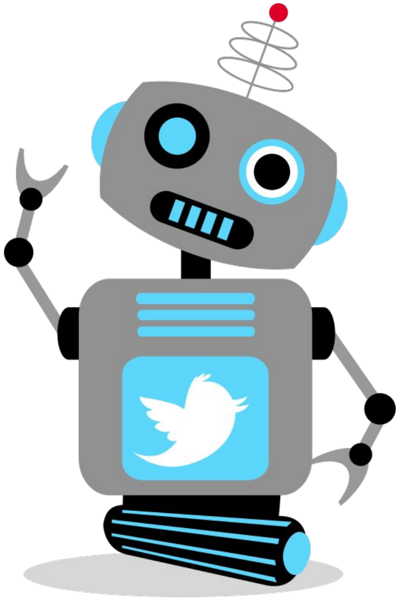


Image © IoActive

TEH ERA OF BOTS

Gen 1: Simple Crawlers With Basic Action

Example: In home scripts,
Detection: Absence of Cookie, etc.



Gen 2: Still Easy to Detection

Example: HTTP load generator such as Vegeta

Detection: Absence of JavaScript

Gen 3: Look Like Browsers, Start of Low and Slow Attack

Example: PhantomJs, Selenium

Detection: Challenge tests and fingerprint

Gen 4: Bots Mimic Human Behavior Such as Non-Linear Mouse Movements

Example: Headless browsers || Cobt, Gen4 bot in ANSI-C (18K), developed by Innovera Tech

Detection: AI based solutions

IRONFOX

Ironfox

- Web Application Layer protection
  - WAF based solutions are not enough
- Real-Time, Distributed & High Performance BOT detection & protection
- Simple & Monolithic
- Light-way & Fully stateless
  - Zero Latency
  - Minimal Configuration
- Integration (Service & Source Code)

NGINX

Service & Protections scope

- Website and online business
- Mobile Applications by AppArmor
  - API & REST services

SERVICE

SERVICE &

PROTECTIONS SCOPE

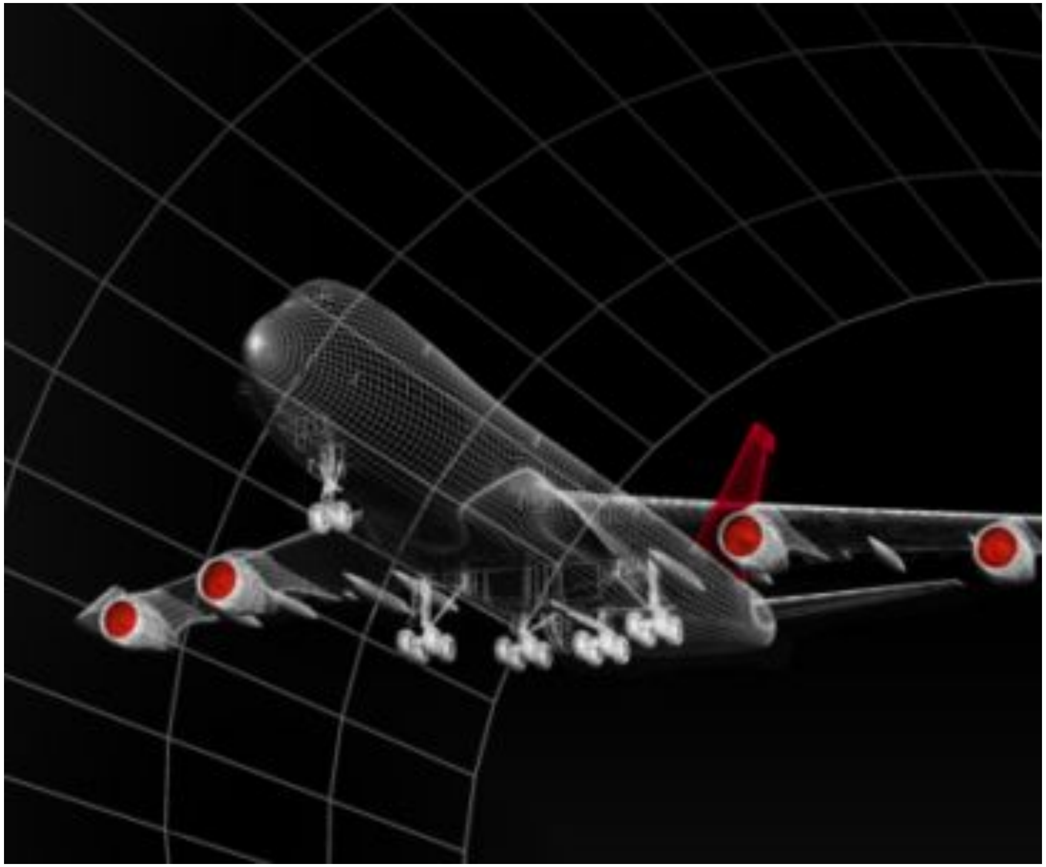


Image © IoActive

REAL-TIME BOT PROTECTION

IronFox Real-Time BOT detection & service

- 100% Transparent & fully works in Agent-Less mod. No additional changes is required in your client or integration with your source code
- Identify & classification of real users vs bots (also determine a good or a bad bots) with tracking and control their activities
- Tracking and control clients by real & unique id
- Complex Web Application Layers (L7) Dos/ DDoS attacks detection & prevention
- Save Your Money. Detection & blocking Ad-Fraudsters
- Blocking automatic vulnerability & security scanners
- Blocking Spammers,Crawlers & unexpected auto/semi-auto clients
- Server & Service overload protection
- And all of BOT activities affected your business and service

REAL-TIME BOT PROTECTION

Ad Fraud Detection

Complex Web Application layer Dos/DDoS attacks Protection

blocking Vulnerability
Scanners

Auto-Fake Account creation
mitigation

Block Scrapers

Backend (Servers) Overload protection

Spam blockers

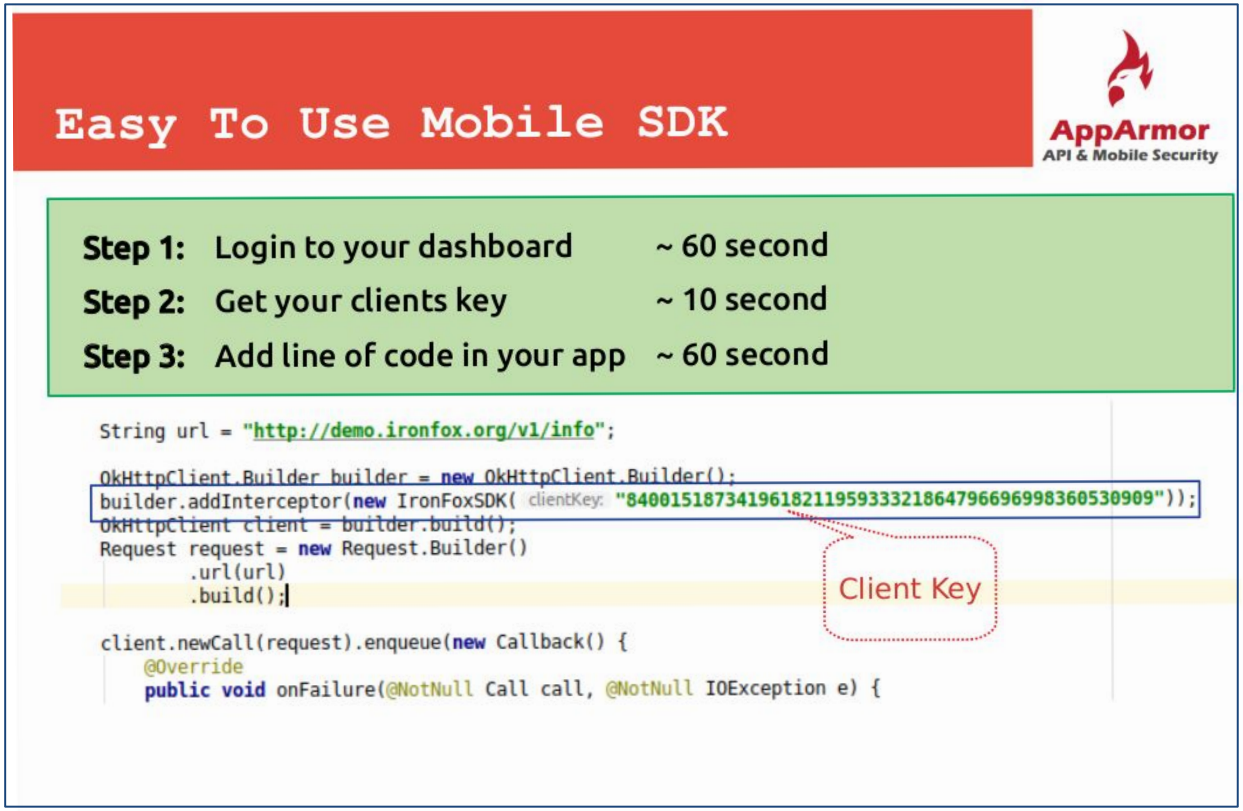
APP ARMOR

Mobile Applications & APIs Protection

- Full API & Real-Time Service Protection
- Mobile Application Cracking, Clone, Malicious code injection detection & protection.
- Tracking & Reporting
- Anti-Debugging & self protection
- Self Destruction Call (SIG KILL)

Easy to use Mobile SDK

- Easy to use API
- Protection with minimal coding



Easy To Use Mobile SDK

Step 1: Login to your dashboard ~ 60 second

Step 2: Get your clients key ~ 10 second

Step 3: Add line of code in your app ~ 60 second

```
String url = "http://demo.ironfox.org/v1/info";

OkHttpClient.Builder builder = new OkHttpClient.Builder();
builder.addInterceptor(new IronFoxSDK( clientKey: "840015187341961821195933321864796696998360530909"));
OkHttpClient client = builder.build();
Request request = new Request.Builder()
        .url(url)
        .build();

client.newCall(request).enqueue(new Callback() {
    @Override
    public void onFailure(@NotNull Call call, @NotNull IOException e) {
```