AdaptiveMobile Signalling Protection
Securing the Network against Privacy & Fraud Attacks
Product Overview

Signalling networks using protocols such as SS7 and Diameter are under attack from adversaries and fraudsters, exploiting loopholes in the protocols to breach subscriber privacy, deny access to key services and to directly defraud mobile operators. Government regulators, corporate customers and consumer organizations are becoming increasingly concerned following a number of high profile exploits. Mobile operators urgently need to implement a signalling firewall and threat intelligence solution to ensure ongoing trust in their networks before their brand, customers, partners and subsequent revenues are negatively impacted.

SS7 was once an obscure protocol protected by a strong ‘walled garden’ of large government-owned telecom providers. With deregulation and the global expansion of mass mobile communications, SS7 access is now commonplace, and entry to the walled-garden can be accessed for legitimate and illegitimate means.

Diameter, a newer signalling protocol used in LTE and IMS is also at risk. Developed with an IP perspective, many more adversaries and fraudsters already possess the knowledge and skills required to carry out security exploits. In addition, access to IP based networks is even more readily available than access to SS7 networks.

AdaptiveMobile Signalling Protection secures the SS7 and Diameter networks using a unique combination of a carrier-grade signalling firewall, advanced reporting and a global threat intelligence service. Therefore, the solution goes well beyond just a signalling firewall, building on AdaptiveMobile’s market leading position in the mobile security industry to block current attacks on the network and to react to emerging threats that seek to bypass standard SS7 and Diameter firewall functionality.

Typical Attacks Prevented
Signalling Protection can secure the mobile network against the following types of signalling-based privacy and fraud attacks:

**Subscriber Location**
- Blocks unauthorized queries for subscriber location data
- Prevents both direct queries for location data and 2-stage queries involving 2 separate transactions

**Call and Data Interception**
- Blocks manipulation of network and subscriber data leading to ‘man in the middle’ attacks
- Secures encryption keys against attack

**Fraud**
- Early detection of protocol anomalies deters and stops fraudsters from exploiting subscriber and network data leading to direct revenue loss

**Denial of Service**
- Secures subscriber data against malicious attacks removing access to key services

Benefits
Monitor and block attacks without major network disruption
- Straightforward and low impact overlay approach enables rapid protection of your network
- Located at strategic network positions to ensure blocking of privacy and fraud attacks

Detects new types of attacks
- Prevents GSMA Category 1, 2 and 3 attacks
- Smart algorithms uncover suspicious activity
- Global Threat Intelligence Service leverages real world intelligence from customer sites on 5 continents

Threat reporting enabling fast and accurate risk assessment
- Dashboard delivers unique insights with drilldown to full details of original source packet

Multiple operating modes allowing a flexible and phased approach
- Passive monitoring, active routing & blocking, or combined mode
The AdaptiveMobile Approach

AdaptiveMobile’s unique three-point defence against Signalling-based threats combines our Signalling Firewall, security-focussed advanced analytics algorithms and reporting, and our global threat intelligence service to ensure network borders are continually secured against the most sophisticated attacks.

Signalling Firewall
Blocks suspicious traffic before damage occurs
• Simply overlays onto existing Signal Transfer Point (STP) network infrastructure
• Placed at signalling Interconnect points to secure network against attacks
• Integrated within a comprehensive approach to deal effectively with the growing problem

Advanced Reporting
Identify and report on threats to the network
• Sophisticated Management and Filtering Engine utilising smart algorithms and traffic analysis
• Flexible and extendable packet analysis to search for Signalling abnormalities
• State-of-the-art Threat Reporting with a built-in Big-Data approach, drill down threat details and actionable insights

Threat Intelligence
Discovery of new and emerging threats
• Extensive expertise in SS7, Diameter and security to deal with emerging signalling threats
• Unrivalled network threat intelligence from over 75 operator deployments globally
• The industry leader in mobile operator network security, protecting over 1.5 billion subscribers worldwide

Network Integration

AdaptiveMobile Signalling Protection can seamlessly fit into existing network flows via probes at the STP for passive monitoring or Opcode routing at the STP for active routing and blocking.
For active routing and blocking only selected commands need to be routed to the platform, ensuring minimum disruption to existing configurations.

In-line deployment in front of the STP is also an option for an operator to consider. Please refer to our Signalling Protection Gateway Product Overview.
Key Features

Attack Analysis
- Identify source & target of security attacks
- Initiate additional preventative measures as necessary
- GSMA Cat 0, 1, 2 & 3 (SS7 & Diameter) stateful detection based on continual real world data analysis and research
- Real time application of rules & filters

Rules Engine
- Sophisticated Rules UI enabling operator admin to configure and customise rules
- Preconfigured rules are validated with real world data from across 5 continents
- Flexible powerful rule definitions across an exhaustive list of fields: MAP/CAP/TCAP/SCCP/Sigtran & Diameter (S6, S9, Sh) interfaces
- Heuristics detection algorithms, node fingerprinting*
- Thresholds on allowed traffic rate per operation type per GT*
- Rules enabling Stateful inspection of SS7 and Diameter traffic

Security Enforcement Point
- SS7 STP access point (inline or adjunct)
- Diameter Edge Agent (DEA) access point (adjunct)
- Inline and adjunct deployment options
- Active and Monitoring operational modes
- Support for MAP, CAMEL, TCAP, SCCP, SIGTRAN, & Diameter (S6, S9, Sh) interfaces

Advantages

Security as a focus
- Leverages the expertise acquired from processing 30 billion security events per day
- Existing knowledge base of threats and attacks can be applied to SS7 and Diameter Firewall
- Community feedback with automatic cartridge updates
- Leading influencers of industry-wide recommendations within major industry bodies for signalling protection in mobile networks

Designed for carriers
- Built by the leading experts in mobile network security
- Proven platform scale handling billions of daily transactions
- Global Threat Intelligence Service leveraging real world intelligence from customer sites on 5 continents

Security Management Console
- Rule & Filter Definition
- Rules UI enabling operator admin to configure and customise rules for each individual packet
- Black and White-List configuration (SS7: GT, Number Plan, OpCode & Diameter: Host and Realm)
- Selection of MAP and CAMEL operations for monitoring
- Configurable Watchlist for defining and monitoring signalling traffic of subscribers of interest

Advanced Threat Reporting
- Customizable Dashboard
- Role-level authentication
- High level view of attacks with drill-down to full details of the original source packet
- Scheduled reports emailed to key stakeholders
- Built-in report suite with customized options
- Streaming SDK enabling third party BI tool integration for deeper interactive investigation and customer driven reports
- Watchlist report for subscribers of interest

Architecture
- Support for geographically distributed signalling firewalls, centralized firewall management and reporting
- Trusted signalling architecture deployed at scale in Tier 1 operators
- Bare metal and virtualized today, future proofing for NFV
- Intelligence sharing with open APIs for external analytics platforms

Future Proof
- New signalling protocols can be added as threats emerge
- Roadmap of planned enhancements across full Network Protection Platform

Risk Free Decision
- AdaptiveMobile has the SS7, Diameter and security real world expertise to deal with the emerging signalling network threats
- By working with the industry leader, you are assured of access to unrivalled market intelligence that can proactively identify and deal with new sources of attacks before they impact your network
- Option to introduce passive monitoring before active blocking

About AdaptiveMobile

AdaptiveMobile is the world leader in mobile security protecting over one billion subscribers worldwide and the only mobile security company offering products designed to protect all services on both fixed and mobile networks through in-network and cloud solutions. With deep expertise and a unique focus on network-to-handset security, AdaptiveMobile’s award winning security solutions provide its customers with advanced threat detection and actionable intelligence, combined with the most comprehensive mobile security products available on the market today. AdaptiveMobile’s sophisticated, revenue-generating security-as-a-service portfolio empowers consumers and enterprises alike to take greater control of their own security. AdaptiveMobile was founded in 2003 and boasts some of the world’s largest mobile operators as customers and the leading security and telecom equipment vendors as partners. The company is headquartered in Dublin with offices in the North America, Europe, South Africa, Middle East and Asia Pacific.

For discussion of typical use cases, overview of AdaptiveMobile’s existing deployments or a full walkthrough of service provider and enterprise experience, contact your local office:

www.adaptivemobile.com/contact-us