Flying Squirrel

WIRELESS DISCOVERY/MAPPING APPLICATION

Flying Squirrel, the approved Department of Defense (DoD) standard tool for real-time wireless discovery and mapping, enhances network security by detecting unauthorized wireless activity.

Key Features

Wireless Discovery

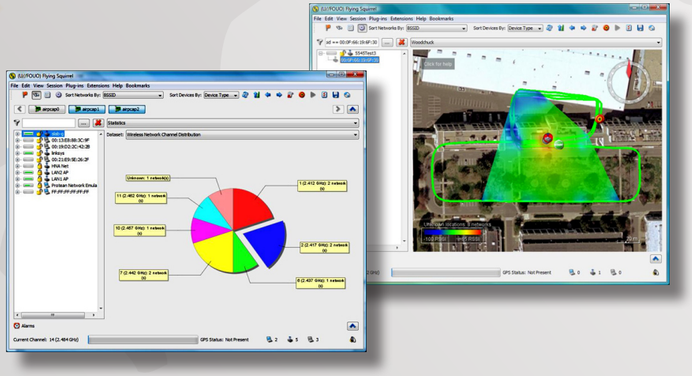
- Easy-to-use graphical interface with both *Windows* and *Linux*
- Supports 802.11a/b/g/n
- Real-time protocol analysis
- Cloaked network discovery
- Arbitrarily filter, search, and sort networks
- Statistical analysis of captured network traffic
- Customizable report generation

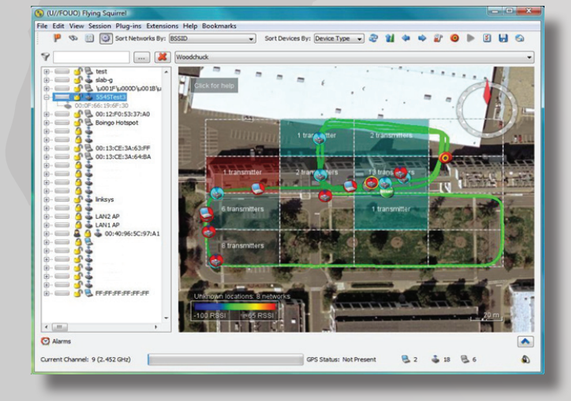
Wireless Mapping

- Real-time signal strength interpolation
- Real-time drive path & logical network visualization
- Integrated Geographic Information System (GIS)
- Google Earth™ export
- Filter networks by geographic area
- Blueprint overlay

With the advantages that wireless technologies provide, many organizations are seeking the means to securely integrate wireless capabilities into their networks. In an effort to standardize wireless security for the purpose of detecting and thus deterring unauthorized wireless activity, the DoD Enterprise-Wide Information Assurance/Computer Network Defense Solutions Steering Group (ESSG) identified the need to enhance network security through the employment of a Wireless Discovery Device (WDD) capability.

Serving as the approved DoD ESSG WDD, the Flying Squirrel Wireless Discovery/Mapping Application is a government-off-the-shelf (GOTS) software application developed by the U.S. Naval Research Laboratory to provide real-time discovery, analysis, and mapping of IEEE 802.11 a/b/g/n wireless networks.





Flying Squirrel is strictly a standalone application designed to run on a standard laptop that is at no time connected to the network. It can be deployed pre-installed on a Linux bootable operating system image or installed on a Windows XP/Vista laptop. Flying Squirrel supports various wireless adapters for collecting traffic and various Global Positioning System (GPS) receivers for recording the geographical coordinates of detected wireless transmitters.

Flying Squirrel also provides an integrated visualization and mapping capability called Woodchuck. Woodchuck allows users to generate an "RF-map" based on signal strength information for any selected transmitter. This map allows users to conduct basic geolocation by visual inspection. Red represents the strongest signal strength, while blue represents the weakest. This map evolves in real time as users are scanning, thus providing a unique capability to operators. Various other visualizations are possible, all assisting the operator in conducting an accurate assessment of the wireless landscape.

As Flying Squirrel collects wireless data, the wireless networks and transmitters can be visualized in real time and overlaid on imagery. The relevant imagery from various sources can be downloaded using an imagery import application that is distributed with Flying Squirrel. Scan results can also be exported to a KML file that can be opened using Google Earth in an off-line mode.

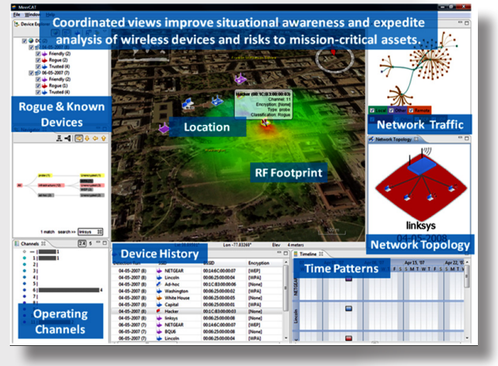
MeerCAT®-FS

ANALYTIC VISUALIZATION TOOL

MeerCAT's visual analytics turn Flying Squirrel's wealth of data into meaningful, actionable information.

Questions MeerCAT helps answer:

- ✓ Are there any unauthorized wireless access points detected within 1 km of the boundaries of the campus or base?
- ✓ Has that SSID been seen near the property within the past month?
- ✓ Has that same SSID been spotted at other, perhaps distant, government sites?
- ✓ Have unauthorized access points connected to the enterprise? To whom did they connect?
- ✓ Are they located within or outside the boundaries of the site?
- ✓ Are our wireless access points encrypted in accordance with our policy?



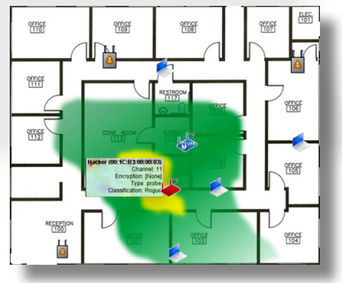
Key Features

- Built-in reporting
- Time trend analysis
- Wireless topology
- Mission correlation
- Communication patterns
- Compares many war drives across locations and time
- Big picture overview; drill-down for detail
- Visual tracks of threat locations: geographic and in-building
- Profile filters highlight suspicious behavior

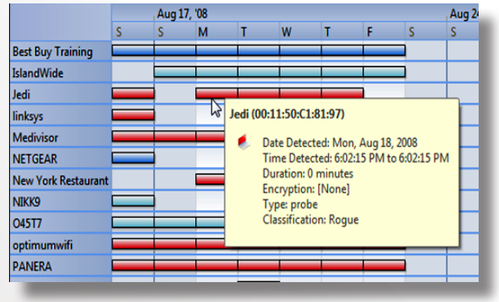
Benefits

- Enhanced threat detection – **Identify hard-to-see patterns in massive volumes of data**
- Less work – **Rapidly analyze many war drives across locations and time**
- Audit trail – **Support compliance reporting**
- Easy reporting – **Create documents and presentations directly from MeerCAT**
- Ease of use – **Get up and running quickly and easily**

MeerCAT's integrated visualization tools help analyze risks to critical assets from mobile threats. It presents a unified picture of location, security state, behavior patterns, temporal patterns, channel usage, and mission of wireless devices. It visualizes communication and movement patterns of wireless threats to help assess the threat's intention and access to high-value targets.



The timeline view shows wireless detections over days, weeks, or even months to help improve network security posture, assist in forensic investigations, and ensure policy compliance.



MeerCAT was developed by the Secure Decisions division of Applied Visions Inc., under DARPA SBIR Phase II Contract W31P4Q-07-C-0022 SBIR Data Rights (DFARS 252.227-7018 (June 1995)) apply.

Caribou

INERTIAL MEASUREMENT SENSOR

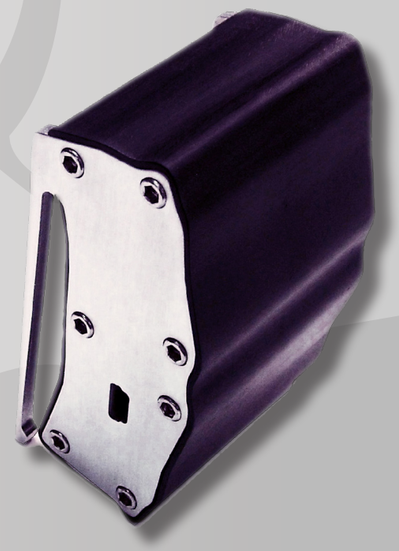
Caribou, an inertial measurement sensor, provides Flying Squirrel position information in the absence of a Global Positioning System signal.

Key Features

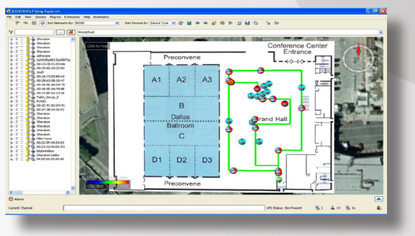
Indoor Tracking

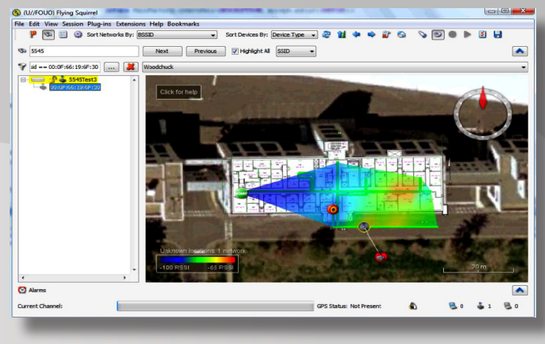
- Inertial, magnetic, and barometric sensors for indoor tracking
- Built-in GPS for outdoor tracking
- Ruggedized enclosure - 3″x 1.25″x 2.5″
- Tilt compensated compass
- USB powered, no need for batteries
- Easily mounts to an operator's belt
- Sensor data is transferred to Flying Squirrel via USB
- Blueprint overlay into Flying Squirrel

To accurately map both known and unknown IEEE 802.11 transmitters in Flying Squirrel, location awareness is essential. In outdoor situations, GPS easily provides this location information. In indoor situations, however, a reliable GPS signal is not likely to be available, thus requiring the user to manually enter position information for collected data points, which is time consuming and limits the accuracy of the transmitter map.



To provide indoor tracking capabilities for Flying Squirrel, the U.S. Naval Research Laboratory developed a GOTS inertial measurement sensor called Caribou that uses inertial, magnetic and barometric sensors to provide position information in the absence of a GPS signal. In order to eliminate the need for two separate devices, Caribou also provides an integrated GPS device for outdoor tracking. Caribou integrates seamlessly with Flying Squirrel, requiring the operator to simply clip the unit to their belt, plug in a USB cable, and for indoor application, pick a starting location.





The **Mobile Systems Security Section**, a component of the Center for High Assurance Computer Systems (CHACS) at the U.S. Naval Research Laboratory, focuses on research and development issues that pertain to the security of modern mobile and wireless communications systems.

Current Projects:

- Next-generation wireless network security
- Geo-location techniques for wireless transmitters
- Mobile ad hoc network security
- Simulation of wireless networks

For Additional Information:
U.S. Naval Research Laboratory
Attn: Code 5545
4555 Overlook Ave., SW
Washington, DC 20375

Fax: (202) 767-1060
Email: 5545info@chacs.nrl.navy.mil
www.nrl.navy.mil/Flying_Squirrel

NAVAL RESEARCH LABORATORY

FLYING SQUIRREL

WIRELESS ASSESSMENT TOOL SUITE

Flying Squirrel

MeerCAT®-FS

Caribou