

Caribou

Indoor Tracking

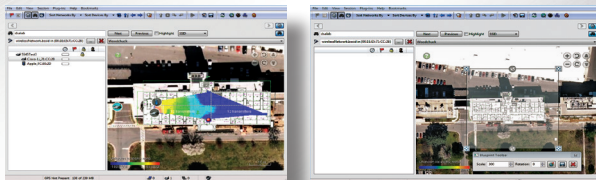
Caribou, an inertial measurement sensor, provides Flying Squirrel™ position information in the absence of a Global Positioning System signal.

Key Features

- 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.

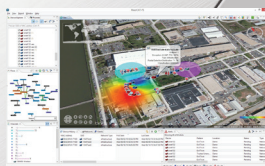
To provide indoor tracking capabilities for Flying Squirrel™, the U.S. Naval Research Laboratory developed a GOTS inertial measurement sensor called Caribou that uses inertial, magnetic and barometric sensors to provide position information in the absence of a GPS signal. In order to eliminate the need 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.



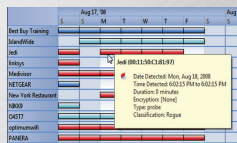
MeerCAT®-FS

Wireless Analysis

The MeerCAT®-FS visual analysis capability identifies threats that pose risks to critical assets from wireless devices. 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®-Flying Squirrel (FS) is a visual analytic capability that analyzes data provided by Flying Squirrel™ into meaningful and actionable information.

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



NAVAL RESEARCH LABORATORY

Center for High Assurance Computer Systems

Flying Squirrel™

WIRELESS DISCOVERY/MAPPING



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. For Additional Information: www.nrl.navy.mil/Flying_Squirrel

www.nrl.navy.mil/flying_squirrel

Flying Squirrel™

Wireless Discovery/Mapping

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

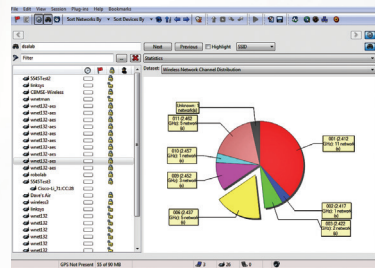
- Easy-to-use graphical interface with both Windows and Linux
- Supports Wi-Fi
- Supports Bluetooth
- Real-time protocol analysis
- Cloaked network discovery
- Arbitrarily filter, search, and sort networks
- Statistical analysis of captured network traffic
- Customizable report generation

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.

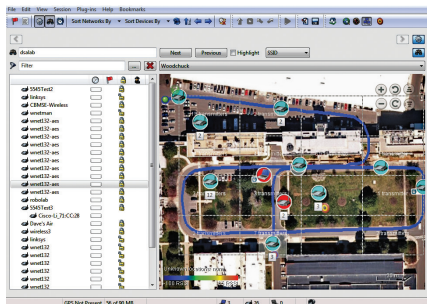
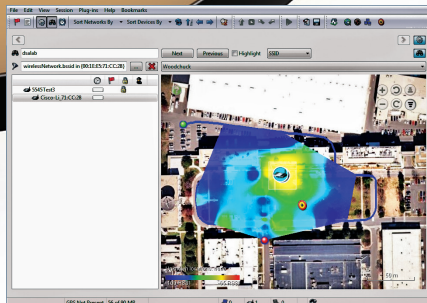
Serving as the approved DoD ESSG WDD, Flying Squirrel™ Wireless Discovery/Mapping Application is a government-off-the-shelf (GOTS) software application developed by the U.S. Naval Research Laboratory to provide real-time discovery, analysis, and mapping of wireless networks.



Flying Squirrel™ is strictly a standalone application designed to run on a standard laptop. It is available as a Windows or Linux application, as well as a Linux bootable operating system image. Flying Squirrel™ supports various wireless adapters for collecting traffic and 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 assist 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™.



Orb-weaver

Persistent Sensor Network



Key Features

- 24/7 Monitoring of area of interest
- Monitoring 802.11 a/b/g/n
- Self-calibrating
- Using economical, low-profile, COTS sensors

Orb-weaver is a dedicated wireless discovery sensor network that utilizes multiple sensors spread throughout the monitoring area. Each sensor independently scans for wireless activity, and when multiple sensor nodes detect device activity, they then coordinate with Orb-weaver to localize it. Orb-weaver then displays the estimated location of the device, along with other visualizations such as radiation fields and data points. The sensor nodes and central instance of Orb-weaver operate on a standalone network segment. Orb-weaver is certified and accredited by the Defense Information Systems Agency (DISA) Designated Approving Authority (DAA) and may be implemented as either a VLAN or a fully physically isolated network.

Ubiquiti UniFi AP / AP Pro Sensors

- Flashed for passive Wi-Fi Discovery
- Supports 802.11 a/b/g/n Wi-Fi standards



Flying Fox (passive Cellular, Wi-Fi, and Bluetooth discovery sensors)

- 24/7 Passive Monitoring, Detection, & Identification of Cellular, Wi-Fi, & Bluetooth devices
- Detects and decodes the Mobile Subscriber Identity (MSI) in transmissions from cellular devices
 - o Zero False Positive cellular detections / identifications
- Automatic cellular survey to determine which cellular technologies (2G/3G/4G) and providers (Verizon, AT&T, etc.) are present.
 - o Periodic cellular surveys can detect changes in the ambient cellular network
- Flexible radio platform to allow updates and upgrades for processing signals between 70 MHz and 6 GHz
- Exceptionally sensitive RF receiver capable of detecting and decoding cell phones transmitting down to -105 dBm
- Provides the following information for every cellular detection:
 - o Cellular technology detected (GSM, CDMA2K, UMTS, or LTE)
 - o Carrier (Verizon, AT&T, T-Mobile, etc.)
 - o RF channel where the detection occurred
 - o Parametrics for the network connection establishment sequence, including the MSI transmitted by the phone

