Passive to Active Operations

- **Primary Goal:** To enable on-net access to target networks via off-net capabilities.
- **Prerequisite:** We need to find the network of interest in order to target it.
- **Procedure:** Conduct passive survey to locate network, then perform active op.
- **Solution:** Utilize BLINDDATE and the appropriate plug-in solution(s).

Passive to Active Operations

- Successful operation of BLINDDATE is essential to correct usage of plug-ins.
- Two types of plug-ins exist:
  - Analysis Tool Aids
  - Active CNE Tools
- We will focus on Active CNE Tools:
  - NIGHTSTAND
  - HAPPYHOUR

Active CNE Assessment

CLOSE ACCESS

- BLINDDATE used as both a survey and vulnerability analysis tool for 802.11 networks.
- Operator needs to know what vulnerabilities, or criteria, to look for in order to utilize the correct Active CNE Tool (if any)
- We will focus primarily on criteria necessary to carry out NIGHTSTAND (NS) and BADDECISION (BDN) operations.

Major Assessment Criteria

CLOSE ACCESS

- **Clients**
  - A client is a prerequisite: If no clients are on the target network, there is nothing to do yet.
- **Security**
  - Encryption setting (Open, WEP, WPA, WPA2) dictates which capability can be used (if any).
- **Signal Strength**
  - SNR dictates whether we can perform a successful active CNE operation.

Active CNE Operations

CLOSE ACCESS

- What does that do exactly?
  - Forces the target to covertly contact a FOXACID server.
- What is FOXACID supposse to do?
  - Perform vulnerability analysis and exploitation of the target (if possible).

Redirection to FOXACID

CLOSE ACCESS

- A FOXACID Tag is a special URL pointing to a particular FOXACID Server.
- Contacting the FA Server will (hopefully) result in the contactor being exploited.
- We want the target to be exploited.
- How do we redirect the target to the FOXACID Server without being noticed.
  - Use NIGHTSTAND or BADDECISION