# Passwords Found on a Wireless Network

## "Don't sue me - honey made me do this"

**Dug Song**
**dugsong@monkey.org**

**University of Michigan CITI**

## Why?

- **Insecure network authentication is just so passe**
- **Virtual tar and feathers: better security through public humiliation**
- **We're not the bad guys, we're the network police (BOFH)**
- **We even eat our own: http://www.citi.umich.edu/dsniff.html**

## How?

- **dsniff - the mother of all password sniffers, plus sniffing tools for penetration testing**
  - **arpredirect**
  - **macof**
  - **tcpkill**
  - **tcpnice**
  - **dsniff**
  - **filesnarf**
  - **mailsnarf**
  - **urlsnarf**
  - **webspy**

## arpredirect

- **Facilitates man-in-the-middle sniffing via ARP spoofing**
- **Enables sniffing on switched networks**
- **Can be used to poison the ARP caches of all, or arbitrary hosts on the LAN**
- **Plays well with others - will restore the original ARP mapping on exit**

## macof

- **Floods the LAN with random MAC addresses**
- **Some network switches fail open in repeating mode**
- **Zen koan: Switch becomes hub, sniffing is good.**

## tcpkill

- **Selectively kills TCP connections**
- **Useful in "initializing" connection state on a LAN for stateful, TCP/IP reassembling sniffers**
- **OK, so maybe this is a little evil**
- **It was just line noise, er, radio interference! Honest!**

## tcpnice

- "You're talking too fast, slow down!"
- Slows down selected TCP connections via "active" traffic shaping (shrinking TCP window advertisements and ICMP source quenches)
- In theory, could be abused to enforce local (unilateral) QoS policy, e.g. to hog bandwidth for my Napster downloads

## dsniff

- **The mother of all password sniffers**
- **Decodes 30 major protocols and their variants: FTP, Telnet, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, NFS, YP, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase and Microsoft SQL**
- **HTTP module also does QUERY_STRING and x-www-form-urlencoded parsing, to catch most CGI-based auth schemes (all major webmail services except Hotmail, unencrypted e-commerce sites, etc.)**

## dsniff (cont.)

- **Supports magic(5)-style automatic protocol detection - telnet on port 3000 won't help you!**
- **Supports full TCP/IP reassembly, and best-effort half-duplex TCP reassembly (in case of lossy sniffing, or asymmetric routing)**
- **Uses Berkeley DB for storage, only saving unique auth info**

## filesnarf

- **Sucks down files sniffed from cleartext NFS v2, v3, UDP or TCP traffic**
- **Practical exploit for theoretical attacks against X11, SSH, PGP**
  - **e.g. ~/.Xauthority, ~/.ssh/identity, ~/.pgp/secring.pgp**
- **CIFS, AFS, you're next**
- **We're working on NFSv4 - here's your motivation**

## mailsnarf

- **Output e-mail sniffed from POP, SMTP traffic in Berkeley mbox format**
- **Supports regular expression matching against mail header and body**

## urlsnarf

- **Output URLs sniffed from HTTP traffic in Common Log Format (e.g. Apache access_log)**
- **Crunch through your favorite log analyzer, determing web surfing trends**

## webspy

- **Watch someone's web surfing in real-time, on your own browser**
- **Fun party trick!**

# Conclusions

- **Wireless and switched networks are still easily sniffed**
- **Insecure network authentication is still widespread**
- **Public humiliation may help**

## Availability

- **dsniff is freely available under a BSD-style license**
  - **http://www.monkey.org/~dugsong/dsniff/**