Heisenberg, Copenhagen, and TCP/IP

Mark C. Langston

The Arms Race

- People sniff.
- People sniff for people who sniff.
- People find ways around being sniffed for sniffing.
- People find ways around the ways around being sniffed for sniffing.

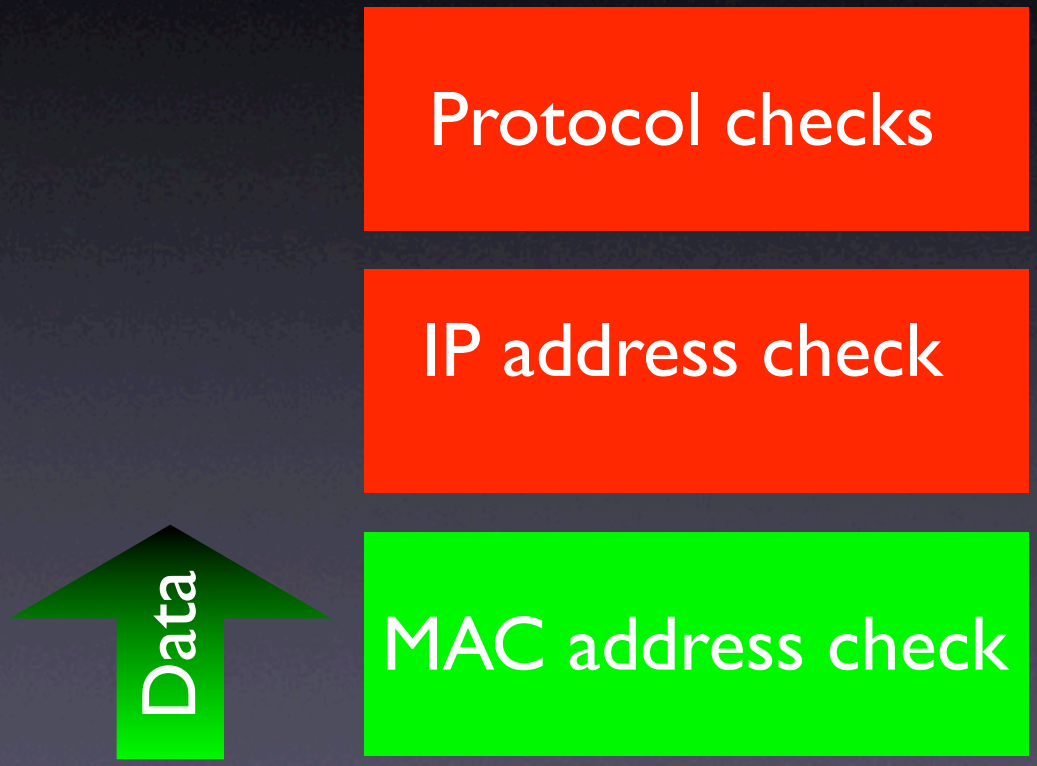
What's a sniffer?

- Promiscuously listens for otherwise-unobtainable signals "on the wire"
- Normal computer, specially-connected computer ("sniffer cable"), wire taps
- Passive v. active sniffers
- Non-invasive v. invasive sniffers

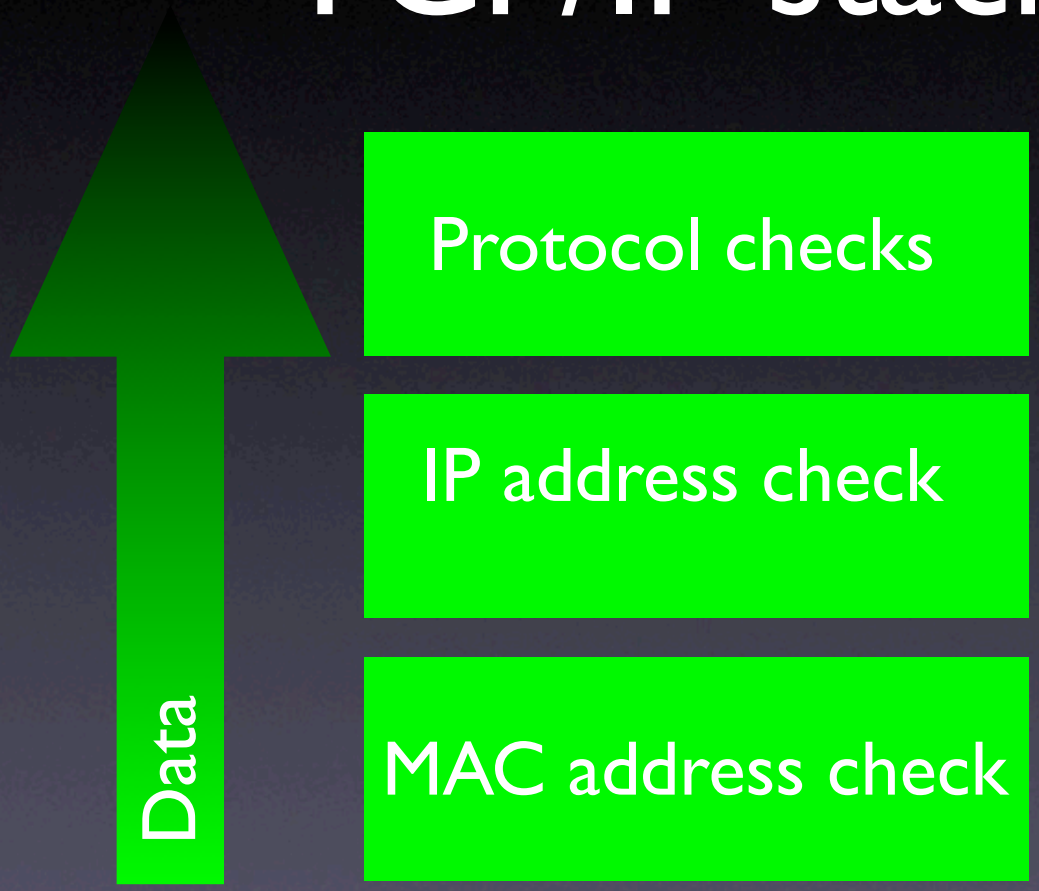
Why sniff?

- Legal reasons: network diagnostics, traffic analysis, hardware testing, protocol debugging
- Illicit reasons: account/password gathering, stalking, reverse-engineering, malicious protocol manipulation

How sniffers work: TCP/IP stack



How sniffers work: TCP/IP stack



Detecting sniffers

- Packet injection techniques:
- “Ping trick”
- “ARP trick”
- “Microsoft trick”

More sniffer sniffing

- DNS resolution
- Latency tests
- Check the media

Evading sniffer detectors

- Disable DNS
- Be smart about ARP
- Prioritize traffic
- Fix your TCP/IP stack!
- Go ***REALLY*** non-invasive - van Eck phreaking!

References

- Sniffer cable - http://www.geocities.com/samngms/sniffing_cable/
- van Eck phreaking - http://www.shmoo.com/tempest/emr.pdf