**Introduction**

* Redirect from a legit http site to an https site is unguarded
* Our goal is to confirm the possibility of such an attack
  + Posed access point or first hop access
* Found to be a problem
  + Possible solutions: Table of standard sites/types of sites that cause browser to auto-redirect. Anything possibly DNS based?

**Related Work**

* Many on phishing type redirect attacks but none would do what we do, that is the url would appear to be exactly what they typed just not an https version.
  + Usually via arp cache poisoning or DNS cache poisoning
* Other work on how redirecting http to https is bad practice (though many sites still do it)

**Adversary model**

* Adversary poses as an access point
* He can catch packets passing by and drop the redirect servicing it himself with spoofing the server.

**Methodology**

* Solutions would require foreknowledge of sites that would standardly do this https redirect.
* Other ideas may include having sites send errors to http with a message saying you must use https instead of redirecting
* Is there a way to add it to the network responsibility?

**Implementations/Experimentation**

* Created a way to capture and alter packets
  + Ideally would filter incoming traffic and look for redirects from target sites

**Conclusion**

* It is a real vulnerability though if the user knew sites should be https then it wouldn’t be an issue.
* Further work would attempt to implement solutions to thwart such attacks

**References**