®

The Printer Working Group

Reported mDNS/DNS-SD Attack Vector

Michael Sweet

Lakeside Robotics

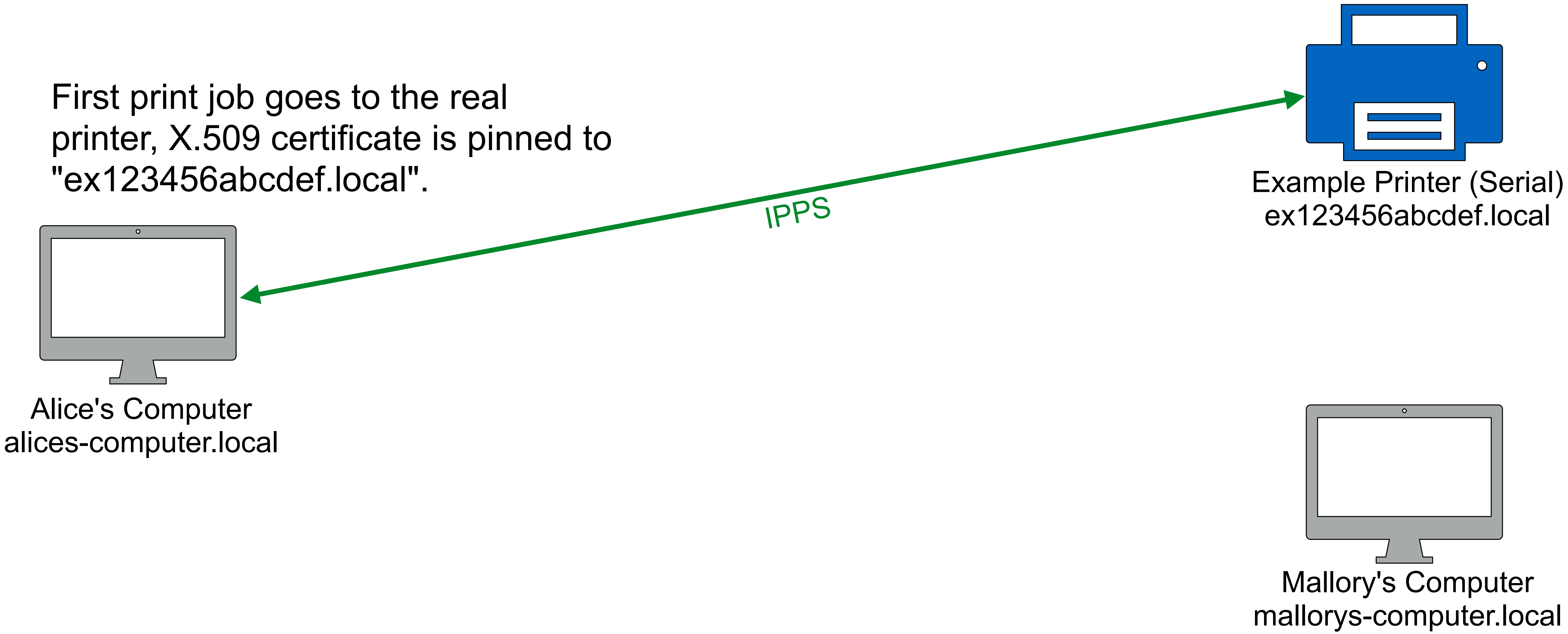
October 10, 2024

mDNS/DNS-SD Attack Vector

- mDNS has a known vulnerability to impersonation attacks
  - A malicious host can hijack a known mDNS hostname and/or service instance name in order to intercept traffic for a network service such as a Printer
- The normal way Clients detect such substitutions is to pin the Printer's X.509 certificate when negotiating a secure (TLS) connection
  - Currently AirPrint and CUPS pin self-signed certificates to the mDNS hostname
  - If an attacker only hijacks the service instance name and points to a new/different hostname, the hostname-based pinning check will fail

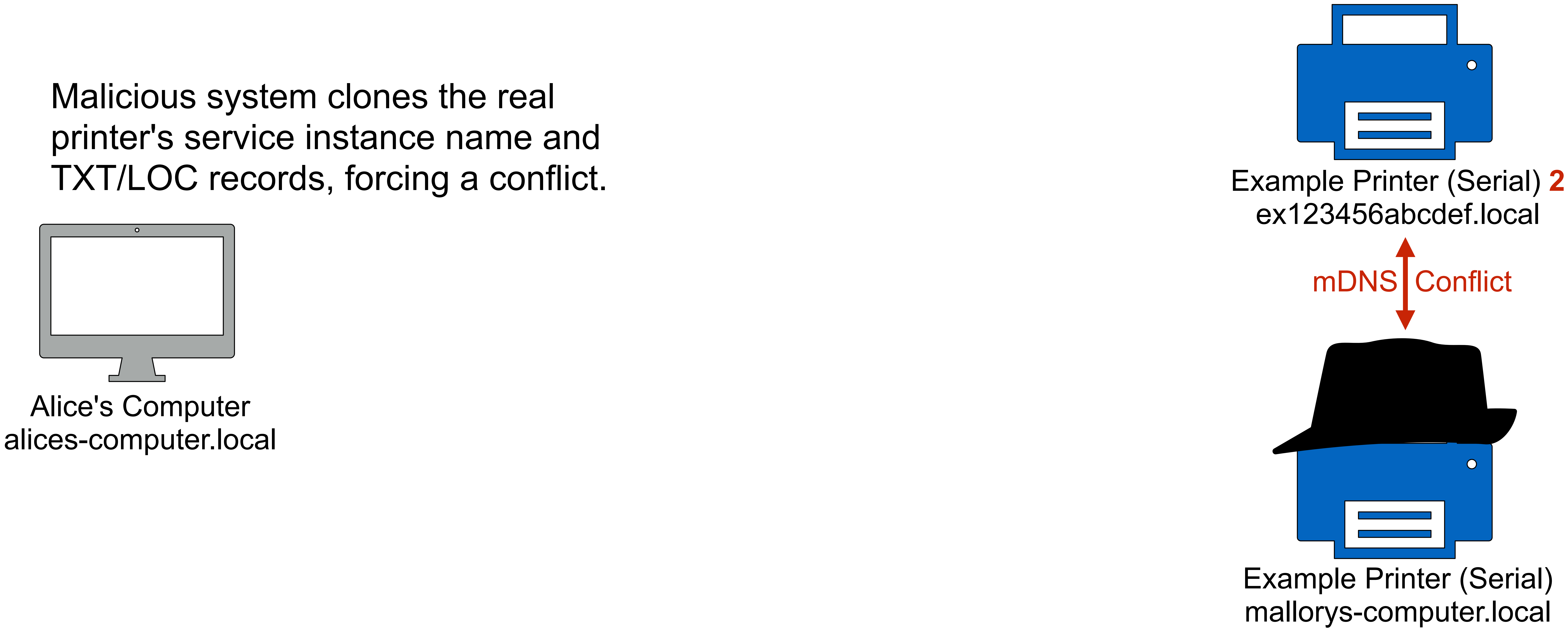
mDNS/DNS-SD Attack Vector

First print job goes to the real printer, X.509 certificate is pinned to "ex123456abcdef.local".



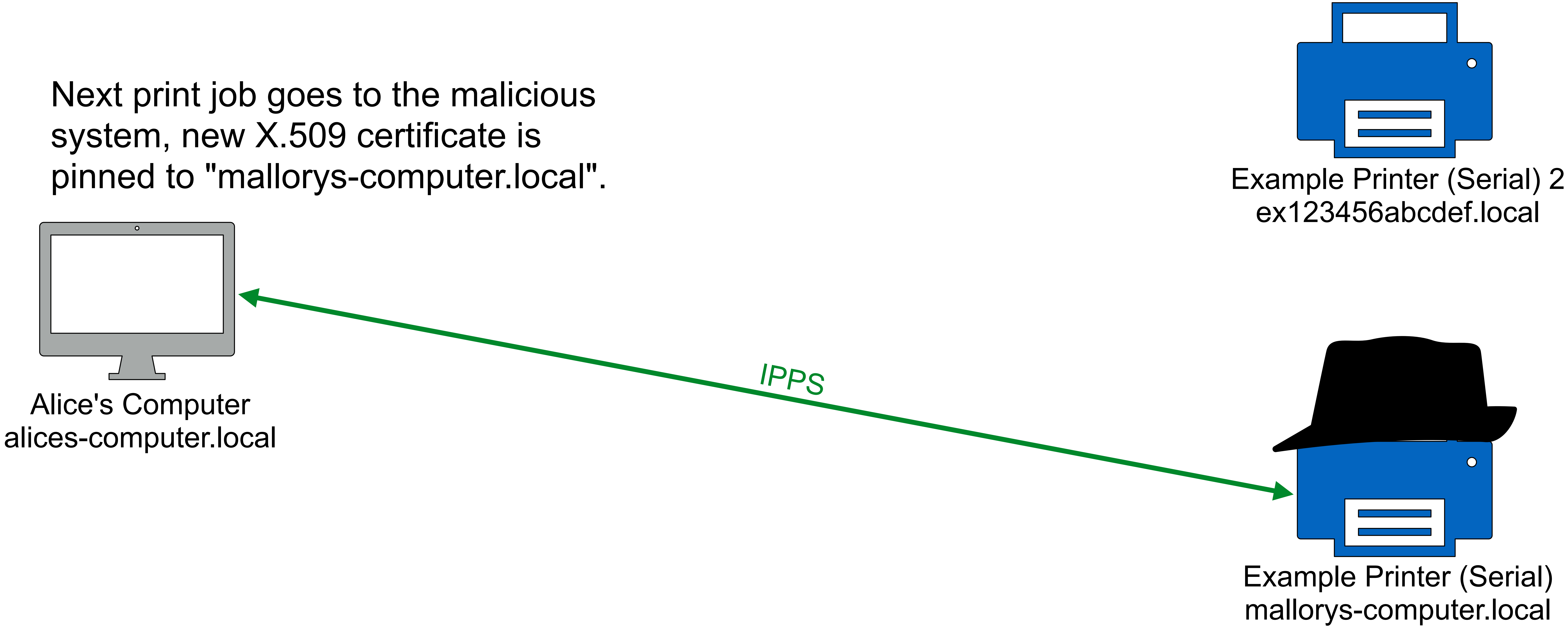
mDNS/DNS-SD Attack Vector

Malicious system clones the real printer's service instance name and TXT/LOC records, forcing a conflict.



mDNS/DNS-SD Attack Vector

Next print job goes to the malicious system, new X.509 certificate is pinned to "mallorys-computer.local".



mDNS/DNS-SD Attack Solutions

- Pin the X.509 certificate to a unique identifier such as the local print queue name or the printer-uuid value
  - Issue: The print queue information is not always available when connecting to the Printer
- Pin the X.509 certificate to a hash of the printer-uri value
  - Issue: Doesn't work for validating Printer resources
- Employ DNSSEC over mDNS to detect changes to hostnames or service instance names
  - Issue: Not widely implemented
- Others?