Access Tokens and Exploits

CS460
Cyber Security Lab
Spring '10

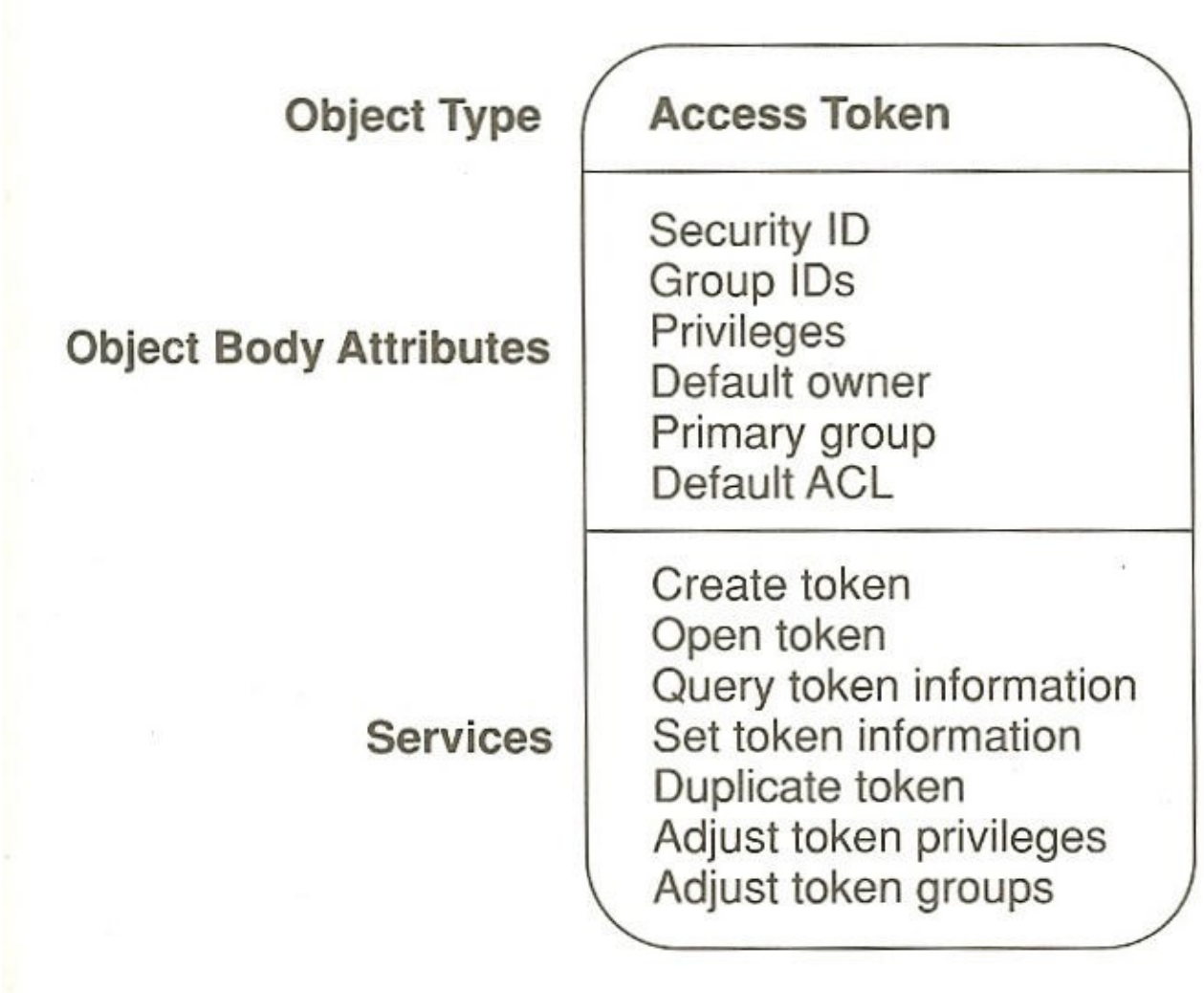
Post-Exploit Actions

- Successfully exploit a process
  - Escalate privilege locally
  - Gain access across domain
- Can leverage knowledge of access tokens to do both
  - Security Implications of Windows Access Tokens – A Penetration Tester's Guide, by Luke Jennings
  - http://labs.mwrinfosecurity.com/files/Publications/mw

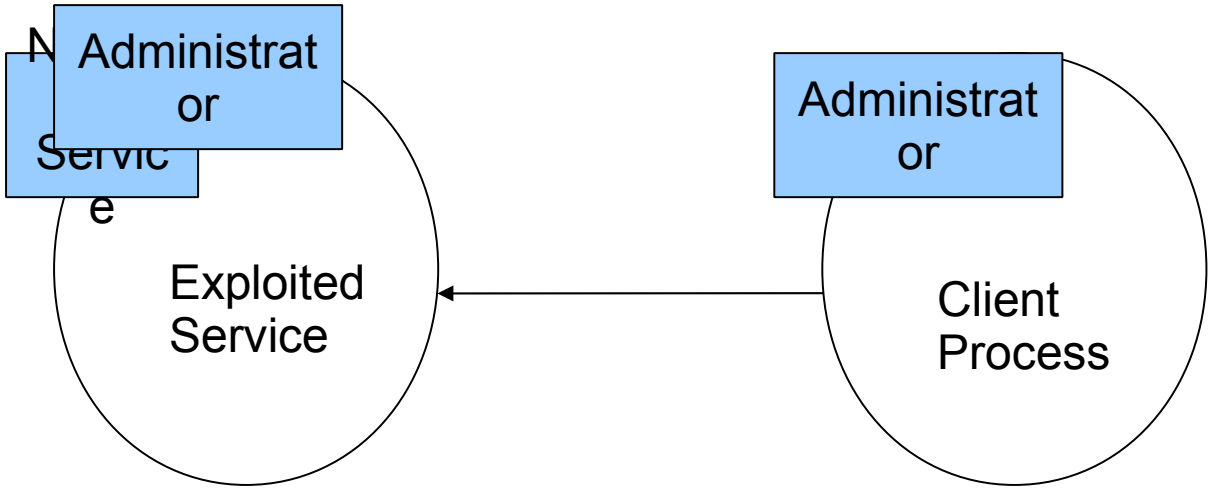
Remember Access Tokens

- Kernel object that contains the security relevant information about a process/thread
  - SID, privileges, integrity level, etc.
- Token per process
- Potentially impersonation token per thread
  - Impersonation token
  - Delegation token

Access Token



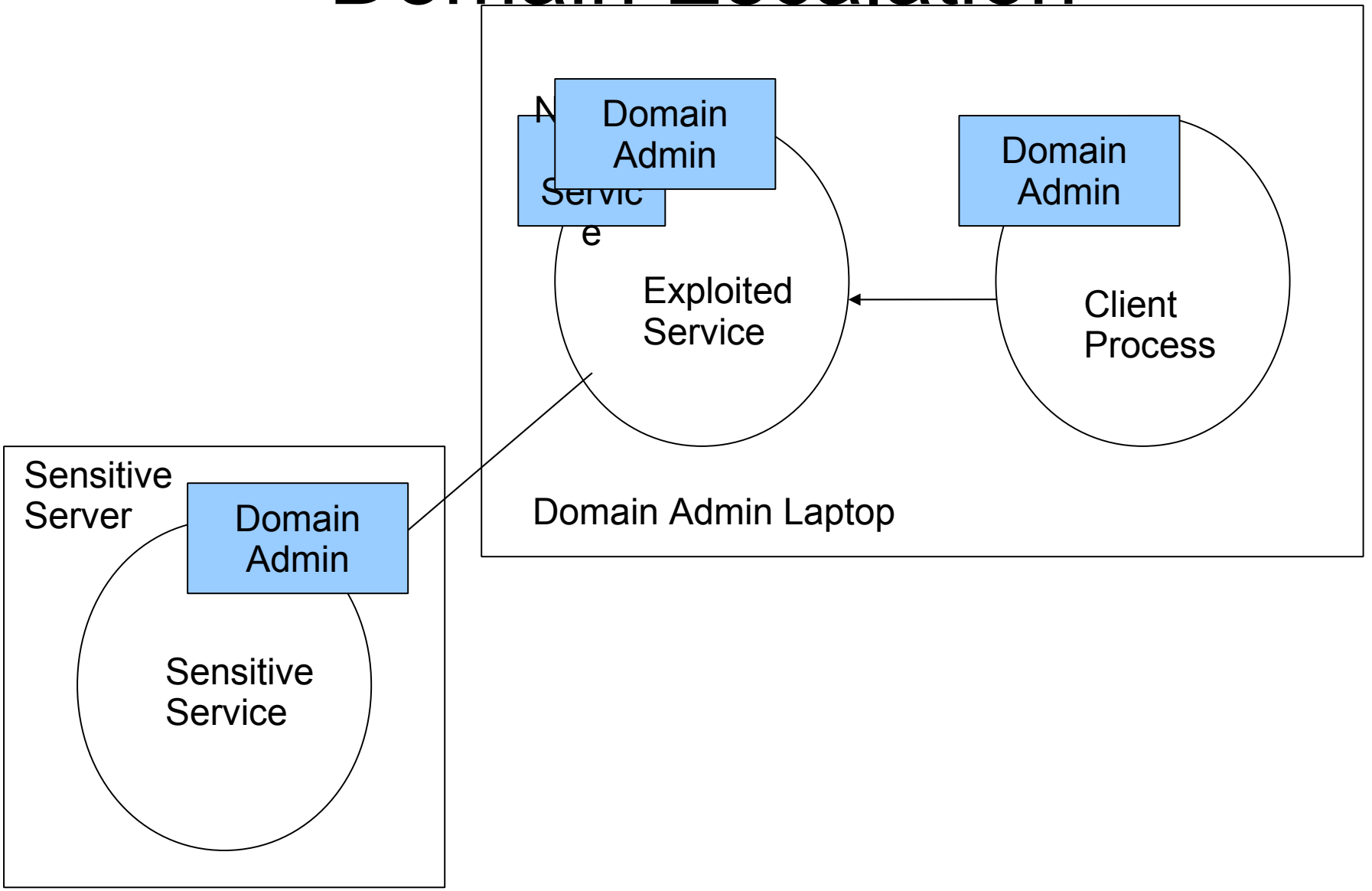
Local Escalation



Local Escalation

- Older versions of windows did not require SeImpersonation privilege
  - Could have even lower privilege services exploited or set up by attacker
- Can perform access checks under Impersonation token
  - Cannot delegate to other processes

Domain Escalation



Domain Escalation

- The Sensitive server isn't misconfigured
- Weakest link in entire domain could cause domain-wide exploit
  - One unpatched test server visited by high privilege user could be problematic

Lingering Tokens

- Bug before Windows 2003 sp1
  - Tokens linger after user logs off. Stay until reboot
  - Reported as impersonation tokens but work fine for delegation
- Terminal service
  - Tokens stay if you close window instead of logging off

Incognito Pen Test Tool

- Find all available tokens
  - List all handles
    - Determine which handles point to tokens
    - Enumerate all attributes of the tokens
      - Users, privileges, impersonation levels

Lessons

- Consider how security elements can be misused
- In a multi-machine environment (i.e., a domain), the security of the entire system must be considered