Session Donation

Alek Amrani
DEF CON 17
About me

- Alek Amrani
  - Longhorn Lockpicking Club
  - UT Austin CS Undergrad
  - UT Austin ISO
This Talk

- TURBO TRAC
  - Not a lot of time, so brevity is the name of the game
  - Presenting an Idea, as well as the thought process behind the formation of the idea

- Questions / Comments / Whatnot
  - Time planned at end for this
Background Info

• Session ID (SID) Attack
  • Session Hijacking
    • Session Fixation
    • Cross-Site Scripting
      • Cross-Site Cooking

• Countermeasures exist
Some common countermeasures taken to prevent session hijacking:
- Use of a long random session key
- Regeneration of SID
- Encrypted transmissions
- Secondary Checks
- Limiting by IP Address, etc.
- Changing SID often
Session Donation

• What is ‘Session Donation’
  • Exactly what it sounds like.
  • Donating your SID to someone else.
  • Very similarly to Session Fixation
    • You need to “fix” the victim’s session to a particular ID
  • Many Session Fixation countermeasures won’t work
    • Only accepting server generated ID’s from a cookie
    • Regenerating SIDs
    • Etc.
  • It’s much easier to give someone your identity rather than stealing theirs
Session Donation

• Are you Insane? Why would I give my info away...
  • Example Scenario:
    • Joe logs into a service and deletes the stored information
    • Joe ‘donates’ his session to Jim
    • Joe tells Jim there were problems earlier, and he’ll need to re-enter his information
    • Jim goes to the page, and inputs his information and saves it
    • Joe can now login as himself, and has Jim’s information
Session Donation

• Issues do exist
  • User does not have to login
    • PEBKAC
      • User training, if any, is usually geared toward being cautious when authenticating
  • 'Single Login' Setups
    • Cooperations, Universities, etc.
  • Connection does not need to be interrupted for this attack vector
    • SSL Certs still valid
Session Donation

- Requirements for Attack
  - Attacker must be able to obtain a SID
    - If the attacker can login/use the service, the attacker can obtain a SID
  - Potentially a large group
  - Attacker needs a way to give away their SID
    - Cross Site Cooking
    - Session Fixation
    - MITM
  - Easier to fix a value with these methods than to steal a value
Session Donation

• Why this is dangerous
  • Many 'Session Hijacking' countermeasures won't work effectively

• The victim is being given a valid SID
  • Many Session Fixation defenses just stop attackers from authenticating with a fixed SID
  • Can you prevent someone from giving away their identity?
  • Can you prevent someone from authenticating as themselves, after giving away their identity?
Session Donation

• Session Hijacking Prevention may even make session donation “safer” for the attacker
  • The attacker will be able to invalidate the “donated” session once the attack has been completed, preventing the victim from removing their stolen information
Prevention

- Hard, but not impossible to prevent
  - The attacker isn’t attacking the SID, but the fact that the SID exists, and is used for authentication
- Prevent XSS
  - Large (largest?) percentage of web vulnerabilities
- Use a different SID generation method
  - IP Address check implemented with SID generation and authentication
    - Use hash of IP as part of SID generation
    - Authentication takes place by regenerating SID and comparing
Questions and Comments

- Ready...GO

- Fun story about the 'about me' image

- Unanswered questions and whatnot, you can probably catch me in the Lockpicking Village
These slides, as well as more info will be available via: obsinisiize.com

I can be reached at: obsinisiize@gmail.com