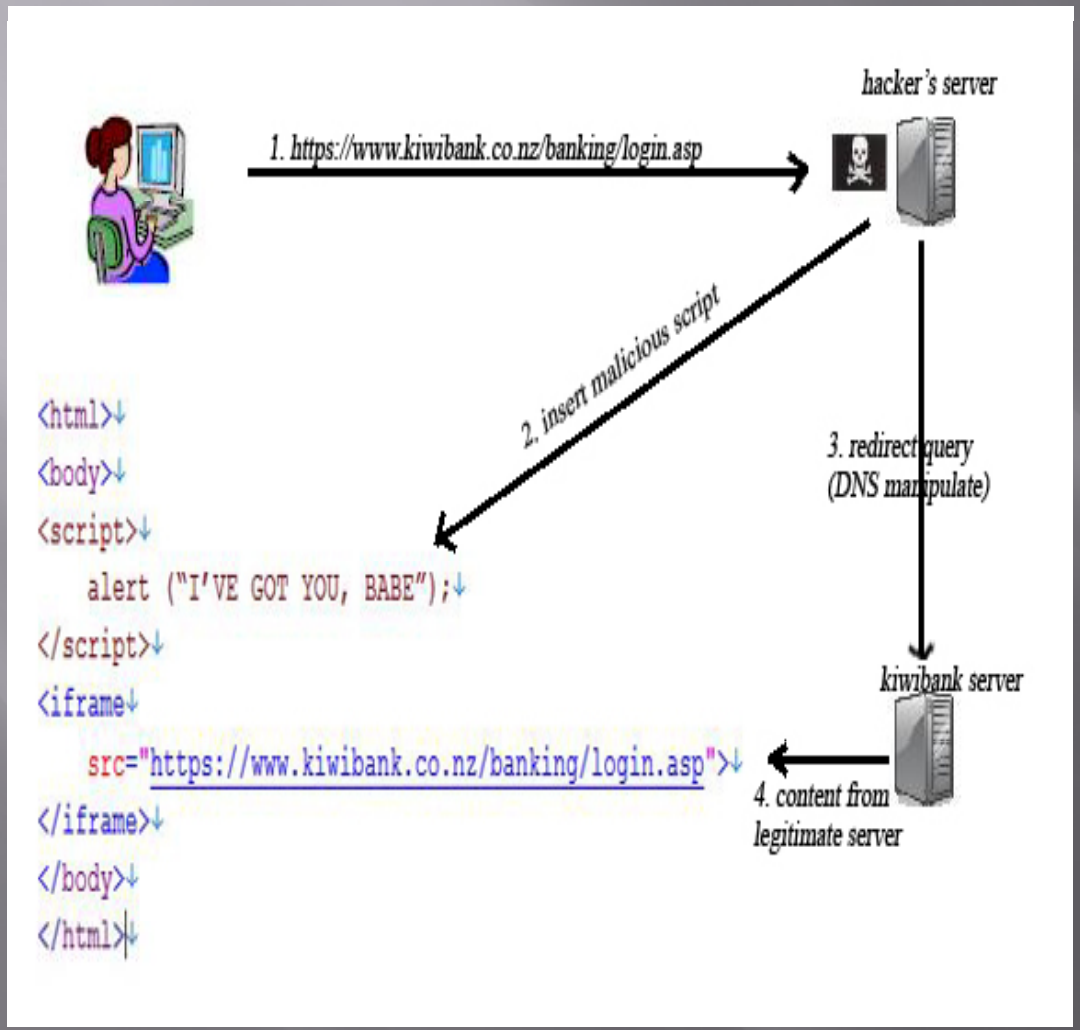
DYNAMIC PHARMING ATTACK & LOCKED SAME-ORIGIN-POLICY (SOP) FOR WEB BROWSERS

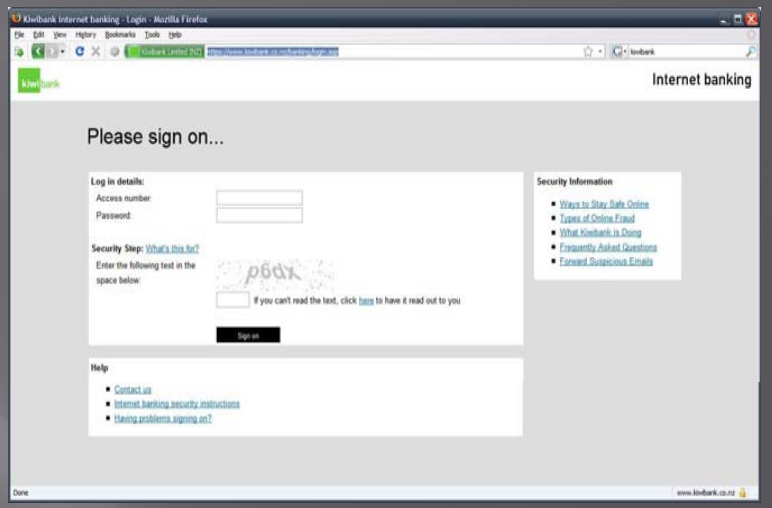
Umesh Shankar, Chris Karlof, J.D. Tygar, David Wagner

(Proceedings of 14th ACM conference – on Computer and Communication Security p.58-71)

Presented by: Huy Van M.

Attack method





Same Origin Policy (SOP)

- Current browsers' implementation of SOP
  - Applicable for 'active' contents
  - Ensure active contents are from SAME domain name + port + protocol
- Weak locked SOP
  - legacy SOP (domain name + port + protocol) PLUS
  - SSL validity bit: invalid when CN/domain name mismatched or self-signed certificate
- Strong locked SOP
  - legacy SOP (domain name + port + protocol) PLUS
  - SSL public key

Deployability

- Challenge:
  - More secure browser
  - Backward compatible
- How are they perform?
  - Weak locked SOP:
    - Low false positive rate (~0.05%)
    - Basic protection, easily to be defeated by a tricky pharmer who can obtain a valid SSL cert.
  - Strong locked SOP:
    - Break several websites (~0.6% false positive)
    - High level protection

Comments

- Implementation is easy
  - Browser developers only need to check the validity of SSL certificates.
  - Better security at minimum cost.
- Cumbersome to apply for websites hosted on multiple servers:
  - web developers need to post SSL public key in a separate file on servers.
- Hacking prevention is limited:
  - Root of the problem: dns manipulation
  - Cosmetics approach: easy to be bypassed by hackers
  - What else can be done?