PROXY BASED ASSERTION

https://www.owasp.org/index.php/Proxyassertion

Erez Kalman
Security Expert
About me

• Over a decade in the IS field
• Don’t have time to publish many articles.. Sorry..
• CISSP-ISSAP, CCSK, Certified Systems Analyst, CCSE, CCSA,....
• My creed: base your decisions on in-depth knowledge but THINK before you allow or cancel an architectural design and use security that works (effective) in terms of mitigating security risks
• I did NOT invent proxy based assertion (PBA)
Proxy based assertion (PBA)

• All communications traverse’s the proxy
• The proxy reads needed http headers (e.g. cookies) and strips them
• Proxy examines target permissions matrix (if needed) to conclude
  • Destination is anonymous access only
  • Destination is secure access only
  • Destination is mixed access
• For non anonymous destinations: authenticate the user, inject assertion headers (username, role/for anonymous only: anon, anon)
• Log and pass-thru to target
• Other architectural designs also possible
Headers from client

- **GET** http://www.areyoureallyreadingthis.com/mybill.htm HTTP/1.1
- Host: www.areyoureallyreadingthis.com
- Proxy-Connection: keep-alive
- User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, sdch
- Accept-Language: en,he;q=0.8
- Cookie: ses=5sdfg199sdfghsvb4fg548fgh02; SID=YAP838OHjhhkgb7M3znWLsp6XbWRm3h-U6WFA9fIGjDXhP5-zgJ6hUVQ
- ASSRT: U=Alice; R=CSR
Proxy action on GET

- **GET** http://www.areyoureallyreadingthis.com/mybill.htm HTTP/1.1
- Host: www.areyoureallyreadingthis.com
- Proxy-Connection: keep-alive
- User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, sdch
- Accept-Language: en,he;q=0.8
- Cookie: ses=5sdfg199sdfghsvb4fg548fgh02; SID=YAP838OHjhjkgb7M3znWLsp6XbWRm3h-U6WFA9fIgjDXhP5-zgJ6hUVQ
- ASSRT: U=Alice; R=CSR
Proxy action after validation

- **GET** http://www.areyoureallyreadingthis.com/mybill.htm HTTP/1.1
- User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, sdch
- Accept-Language: en,he;q=0.8
- Cookie: ses=5sdfg199sdfghsvb4fg548fgh02; SID=YAP838OHjhjkgb7M3znWLsp6XbWRm3h-U6WFA9fIgjDXhP5-zgJ6hUVQ
- ASSRT: U=Bob; R=Customer
Proxy based assertion

Erez Kalman
Proxy based assertion (PBA)

• May, obviously, be used with external authority
• Can be implemented using Apache, mod_sec, mod_proxy or off-the-shelf solutions from Oracle, IBM, etc..
• Used WW by large enterprises (Telco’s, Banks,...)
IBM WebSEAL Junction

- Secure Domain
  - authorization service
    - 3. Authorization check
  - authorization policy
  - protected object space
  - resources

- Flow Diagram:
  - 1. Request
  - 2. Request for authorization (authAPI)
  - 3. Authorization check
  - 4. Authorization decision (authAPI)
  - 5. Authorized operation
  - 6. Response

Proxy based assertion | Erez Kalman
You should still...

- Have multiple layers (defense in depth):
  - Two Firewalls (if possible, one as a bare minimum)
  - WAF
  - Change control for security components
  - SIEM
  - And more..

- OWASP top 10 & SANS 20 recommendations
- TLS 1.2 with client certificate between servers
- Have proper network, and other aspects, secure
What if nothing exists and we're all in somebody's dream?
What if..

- The firewall is misconfigured
  - This would be a network breach, network must be properly engineered
- What if the firewall is breached
  - Use a better firewall 😊
  - Use multiple firewall’s from different vendors
- What if the proxy is breached
  - Best practices need to be in place, in any implementation, latest versions (fully patched) must be in place
  - WAF is recommended
  - Use secure repository for credentials
  - Make sure proper hardening is in place including, where possible SELinux / AppArmor
  - FIM is recommended
What if..

• A malicious administrator performs ARP poisoning or..
  • This would be a network breach, network must be properly engineered
  • Staff hiring and fraud procedures should handle this...

• Why shouldn’t we use SAML ?
  • I am in no way suggesting SAML should not be used!
  • Not all solutions support SAML
  • Proxy can be used for SAML login and achieve SSO
  • SAML has some recurring periodic administrative overhead
  • System to system via SAML is difficult and as such one of the following is usually used
    • No authentication
    • Static username and password
    • Client certificate
    • HMAC
    • PBA is another option – support PBA and no additional method is needed
Pro’s
- Low CR cost
- Single management location for authentication methods
- SSO
- Single access point to DC
- Back-ends supporting SAML can continue using SAML
- No recurring periodic process required

Con’s
- Not all solutions support header parsing – CR cost (usually very low)
- May open a door for malicious employee’s if not properly engineered
- PBA concept is not well known as other techniques, but is widely used WW in large enterprises (banks, telco’s, ...)
- Proxy and backend systems must be properly secured
Q & A
Thank You