

Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers

Based on paper by Chris Karlof, Umesh Shankar, J.D. Tygar, David Wagner
University of California at Berkeley

S.M. Mohsin Reza

Systems Engineering Group
Dresden University of Technology

Winter Term 2008

s0406622@inf.tu-dresden.de

Outline

- ❑ Introduction
- ❑ Motivation
- ❑ Background
- ❑ Locked same-origin policies
- ❑ Dynamic Pharming Attacks
- ❑ Summary
- ❑ References

Part - I

Presentation

Introduction

- **Dynamic pharming** is a DNS poisoning attack that lets an adversary bypass web authentication by waiting until authentication is complete, then modifying the DNS record to hijack the user's session.

-- Source: Umesh Shankar, Google Inc., New York, USA.

Introduction

- ❑ Adversary delivers malicious Javascript
- ❑ DNS rebinding vulnerabilities in browsers
- ❑ Force to connect the legitimate server
- ❑ Adversary waits for the victim to authenticate
- ❑ Hijack the victim's authenticated session

Motivation

- ❑ A locked same-origin policy in the browser can prevent dynamic pharming attack for SSL-enabled servers as well as phishing and active attacks.
- ❑ Authentication mechanisms, Client-side SSL and SSL-only cookies resist both pharming and strong active attacks.

Phishing and Pharming

- **Phishing** is a criminal mechanism employing both social engineering and technical subterfuge to steal consumer's personal identity data and financial account credentials [2].
- **Pharming** is an attack in which a user can be fooled into entering sensitive data into a malicious web site that impersonates a legitimate web site [5].

Same Origin Policy

- ❑ Origin refers to the domain name, port, and protocol
- ❑ Essential security measure for client-side scripting
- ❑ Restriction

URL	Outcome	Reason
http://www.tu-dresden.de/dir2/other.html	Success	Same protocol and host
http://www.tu-dresden.de/dir/inner/other.html	Success	Same protocol and host
http://www.tu-dresden.de:81/dir2/other.html	Failure	Same protocol and host but different port
https://www.tu-dresden.de/dir2/other.html	Failure	Different protocol
http://en.tu-dresden.de/dir2/other.html	Failure	Different host
http://tu-dresden.de/dir2/other.html	Failure	Different host

Table 1: Same origin comparisons [4].

- ❑ Manipulating browser windows, frames, documents, cookies, XMLHttpRequest

Locked Same-Origin Policies

- ❑ Upgrade browser's sop to resist dynamic pharming
- ❑ Use SSL and X.509 certificates
- ❑ Propose two locked SOPs
 - Weak locked SOP
 - ❑ Isolates a domain's locked web objects with valid certificate chains
 - Strong locked SOP
 - ❑ Enforces access control using cryptographic identity

Weak Locked SOP

- ❑ Locked web objects retrieved
 - A legitimate server
 - A pharmer spoofing the server's domain name
- ❑ If certificate warnings ignore
 - Locked web objects allows access
- ❑ Augments the legacy SOP by tagging each locked web object with a validity bit
- ❑ A locked web object to access another locked web object
 - Legacy SOP would allow access
 - Validity bits match

Strong Locked SOP

- ❑ Browsers augment the legacy SOP by tagging each locked web object with public key
- ❑ A locked web object to access another locked web object
 - Legacy SOP would allow access
 - associated public keys match
- ❑ Associating public keys
 - when subject's public key unexpectedly changes

Locked SOP vs Legacy SOP

Policy	Information used to enforce access	Strongest threat model protected against for:		
		Locked web objects	Shared locked web objects	Untrusted certs
Legacy SOP	Protocol, domain, port	Phishers	Phishers	Phishers
Weak locked SOP	Protocol, domain, port, validity of cert chain	Active attackers	Phishers	Phishers
Strong locked SOP (w / policy files)	Protocol, domain, port, server public key	Active attackers	Active attackers	Active attackers

Table 2: Comparison of locked same-origin policies vs legacy same-origin policy [1].

Threat Models

- Phishers
 - Full control of a web server
 - Send emails and instant messages to potential victims
 - Mount application-layer man-in-the-middle attacks
- Pharmers (Phishers +)
 - Change DNS records for the target site
- Active attackers (Pharmers +)
 - Control the Internet routing infrastructure and re-route traffic destined
 - Eavesdrop on all traffic
 - Mount active, network-layer, man-in-the-middle attacks

SSL and X.509 Certificates

- ❑ SSL and its successor, TLS are establishing end-to-end secure channels
 - SSL use X.509 certificates
 - X.509 contains the server's public key
- ❑ Client's browser verify the server's certificate
 - Every certificate in the chain has a valid signature and not expired
 - CN field of 1st certificate matches domain name
- ❑ Participates in a cryptographic protocol
 - Private key corresponding to public key
 - Negotiate a session key to encrypt and authenticate

Dynamic Pharming Attacks

- ❑ Static pharming attack
 - Return the adversary's IP address
- ❑ Dynamic pharming attack
 - Return either legitimate server's IP or its own IP
- ❑ Enables an adversary to compromise all known authentication schemes

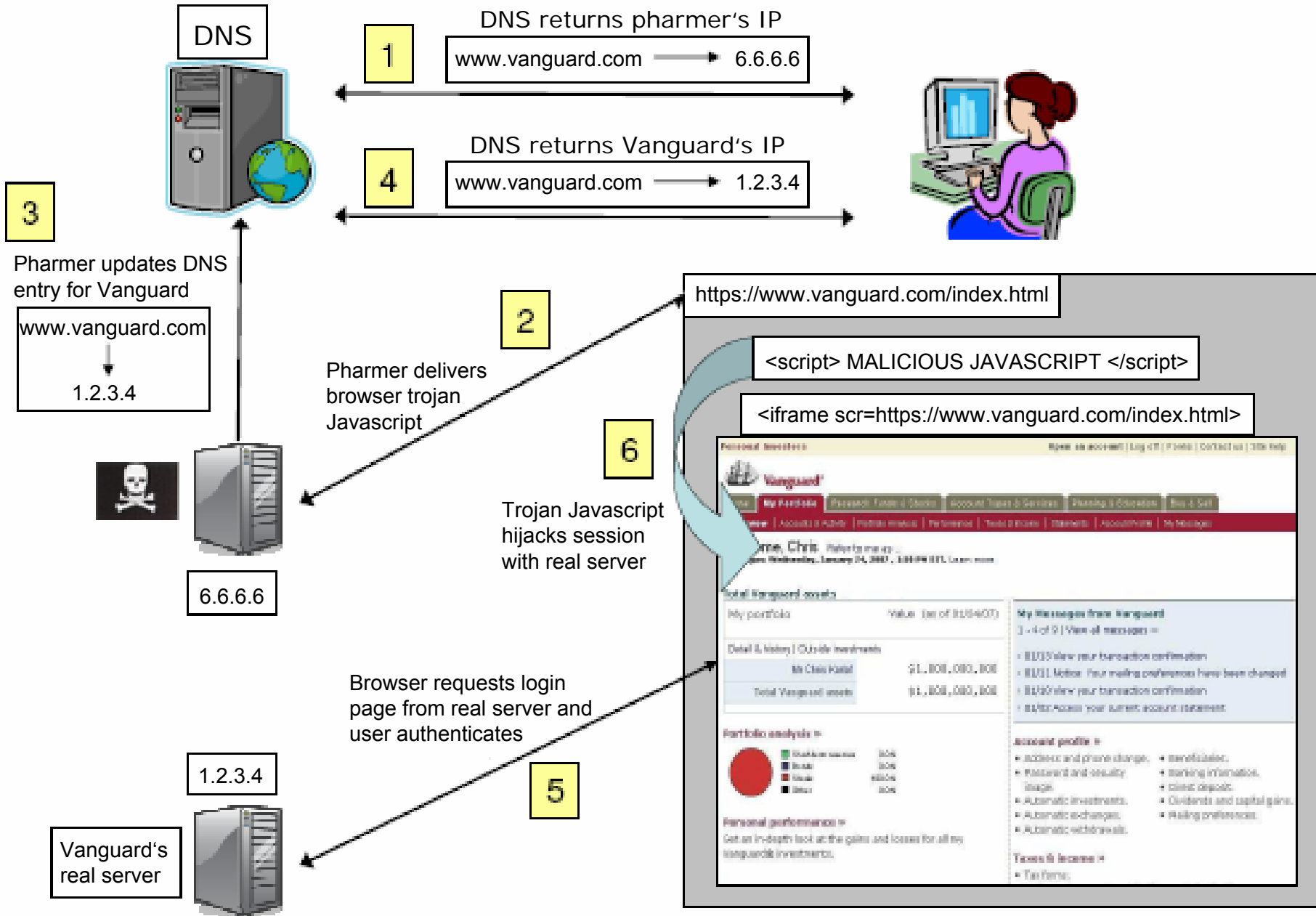


Figure 1: A dynamic pharming attack against www.vanguard.com [1].

Round Robin DNS

- ❑ Pharmers use round robin DNS entries to make attack scalable
- ❑ Load balancing or automatic failover of web sites
- ❑ Round robin DNS entry containing two IP address
 - Pharmer's IP
 - Legitimate server's IP

Security Analysis

- ❑ Weak locked sop
 - Resisting phishing, pharming, and active attacks
 - ❑ A valid X.509 certificate
 - If invalid X.509 certificate
 - ❑ Resists phishing attacks
 - ❑ Don't resists pharming, and active attacks
- ❑ Strong locked sop
 - Resisting phishing, pharming, and active attacks
 - ❑ A valid X.509 certificate with public key PK
 - Try to establish an SSL connection by presenting a X.509 certificate with PK
 - ❑ Resists phishing attacks
 - Adversary doesn't know private key for PK
 - ❑ Cancel the SSL connection

Deployability Analysis

- ❑ An SSL server survey
 - Excluded top-level domains
 - ❑ com, org, net, gov, edu, biz, info, and name
 - 14651 fully qualified SSL domains from 6192 domains
 - 1464 resolved to multiple IP from 14651 domain names
- ❑ Certificate chain validation: Firefox and IE

Browser	Session caching of CA certs	Persistent caching of CA certs	Uses AIA
IE	√	√	√
Firefox	√		

Table 3: Address missing and expired intermediate CA certificates [1].

- ❑ Evaluation results

Policy	Percentage of potentially non-interoperating domains
Weak locked SOP	0.05%
Strong locked SOP	0.6%

Table 4: Deployability analysis of the locked same-origin policies using 14651 SSL domains [1].

Locked SOP Support

- ❑ Multiple keys and key updates
- ❑ Subdomain object sharing
- ❑ Key revocation
- ❑ Active objects
 - YURLs
 - Extending the locked SOPs
- ❑ Caching and dependent elements

Limitations

- ❑ Installing malicious software
 - Executable malware, ActiveX plugin or browser extension
- ❑ DNS rebinding weaknesses in third-party browser plugin implementations
 - Flash, Java, and Adobe Reader
- ❑ Don't address problems
 - Javascript Prototype Hijacking
 - Cross-side scripting (XSS) vulnerabilities in servers
 - Cross-site request forgery (XSRF) attacks

Applications to Web Authentication

- ❑ Web authentication problem
 - Initialization of user's authentication credentials
 - Use credentials to authenticate users to web sites
- ❑ Client-side SSL and SSL-only cookies
 - Locked SOP to resist pharmers and active attackers [3]
- ❑ Registration problem
 - Phishers and pharmers use man-in-the-middle

Summary

- ❑ Hijack user's authenticated web sessions
- ❑ Enables an adversary to eavesdrop on sensitive content
- ❑ Introduced two locked same-origin policies
 - Weak locked SOP (X.509 certificates)
 - Strong locked SOP (public keys)
- ❑ Policies are restrictive than legacy SOP
 - Deny access to an attacker – never the legitimate server
- ❑ Evaluated the security and deployability of approaches

Part - II

References

References

- [1] Karlof, C., Shankar, U., Tygar, J.D., Wagner, D.
Dynamic Pharming Attacks and Locked Same-Origin Policies for Web Browsers.
ACM CCS 2007, pp. 58-71. ACM Press, New York (2007)

- [2] Anti-phishing working group.
Phishing Activity Trends Report, Q1 2008
<http://www.antiphishing.org/>

- [3] Karlof, C., Shankar, U., Tygar, J.D., Wagner, D.
Locked cookies: Web authentication security against phishing, pharming, and active attacks
Technical Report, University of California at Berkeley

- [4] JavaScript Security in Communicator 4.x
<http://developer.netscape.com/library/documentation/communicator/dynhtml/index.htm>

- [5] Pharming.org
<http://www.pharming.org/index.jsp>

Part - III

Thanks for being with me!

Questions?