

VALIDATING UPDATES TO DOMAIN NAME SYSTEM RECORDS

[0001] This application claims priority to US Patent Application Number 12/782,227 entitled "Validating Updates to Domain Name System Records" filed on May 18, 2010, which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] A hierarchical naming system known as the Domain Name System (DNS) allows computers, services, or any resource connected to the Internet or a private network to be referred to by names, such as www.foo.com. DNS servers cooperate to translate domain names that are meaningful to humans into numeric addresses that are used for computer-to-computer communication.

[0003] DNS servers can be targets of "domain jacking," whereby an attacker hijacks control of a domain name. Conventional security measures for DNS servers do not provide a robust defense against domain jacking. In the simplest form of attack, an administrator's account credentials are guessed, or gained via a man-in-the-middle attack by way of malware on the administrator's computer. Once these credentials have been compromised, attackers can then modify records used by the DNS servers to direct traffic for the domain elsewhere, such as a propaganda website or a phishing website.

SUMMARY

[0003a] According to a first aspect of the present invention, there is provided a non-transitory computer-readable medium embodying a program executable in a computing device, the program comprising: code that authenticates a domain owner for purposes of domain name system (DNS) record modification using a first mechanism of authentication; code that receives a request to modify at least one DNS record associated with a first domain owned by the domain owner; code that validates the request by applying at least one policy to the request, the validation responsive to success of the authentication, the at least one policy prohibiting modifications of the DNS record that refer to an identifier that is outside of an infrastructure controlled by the domain owner while permitting modifications of the DNS record that is part of the first domain when the modified DNS record is part of a second domain also owned by the domain owner; code that denies the request to modify the at least one DNS record responsive to failure of the validation; code that authenticates the domain owner for purposes of policy configuration using a second mechanism of authentication for the domain owner, wherein the second mechanism of authentication for configuring the at least one policy is different than the first mechanism used for DNS record updates; code that receives a request to configure the at least one policy; and code that denies the request to configure responsive to failure of the authentication for purposes of policy configuration.

[0003b] According to a second aspect of the present invention, there is provided a system, comprising: at least one computing device; and a domain name system (DNS) policy manager executable in the at least one computing device, the DNS policy manager comprising: logic that validates request a request to modify a DNS record associated with a domain owned by a domain owner by applying at least one policy to the request, the validation responsive to success of authentication of the domain owner, the policy prohibiting modifications of the DNS record that point outside of an infrastructure controlled by the domain owner while permitting modifications of the DNS record that is part of the domain when the modified DNS record is part of a second domain also owned by the domain owner; logic that selectively grants a requested modification to the at least one DNS record based at least upon an application of the at least one policy; and logic that authenticates the domain owner for purposes of policy configuration using a different second mechanism of authentication for the domain owner.

1

[0003c] According to a third aspect of the present invention, there is provided a computer implemented method, comprising: receiving, in a computing device, a request to modify at least one domain name system (DNS) record associated with a first domain owned by a domain owner; comparing, via the computing device, the request to modify the at least one DNS record with at least one policy, the at least one policy prohibiting modifications of the at least one DNS record that point outside of an infrastructure controlled by the domain owner while permitting the request to modify the at least one DNS record that is part of the first domain when the modified at least one DNS record is part of a second domain also owned by the domain owner, the at least one policy being configurable by the domain owner; selectively granting, via the computing device, the requested modification to the at least one DNS record based at least upon the comparison; and authenticating, via the computing device, the domain owner for purposes of policy configuration using a different second mechanism of authentication for the domain owner.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Many aspects of the present disclosure can be better understood with reference to the following drawings. The components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly

CLAIMS

Therefore, the following is claimed:

1. A system, comprising:
at least one computing device; and
a domain name system (DNS) policy manager executable in the at least one computing device, the DNS policy manager comprising:
logic that applies at least one policy to at least one DNS record associated with a domain owned by a domain owner, the policy prohibiting modifications of the DNS record that point outside of infrastructure controlled by the domain owner; and
logic that selectively grants a requested modification to the at least one DNS record based at least upon the application of the at least one policy.
2. The system of claim 1, the DNS policy manager further comprising logic that configures the at least one policy responsive to a configuration request by the domain owner.
3. The system of claim 1, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon an IP address in the at least one DNS record being contained within at least one range specified by the at least one policy.

4. The system of claim 1, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon a name in the at least one DNS record being part of another domain also owned by the domain owner.

5. The system of claim 1, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon a name in the at least one DNS record being within the infrastructure controlled by the owner.

6. The system of claim 1, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon a name in the at least one DNS record being contained within a whitelist specified by the at least one policy.

7. A method, comprising the steps of:
receiving a request to modify at least one domain name system (DNS) record associated with a domain owned by a domain owner;
comparing the request to modify the at least one DNS record with at least one policy, the at least one policy being configurable by the domain owner; and
selectively granting the requested modification to the at least one DNS record based at least upon the comparison.

8. The method of claim 7, further comprising the steps of:
configuring the at least one policy responsive to a configuration request by the domain owner.
9. The method of claim 8, further comprising the steps of:
authenticating the domain owner for purposes of policy configuration; and
denying the configuration request responsive to failure of the authentication.
10. The method of claim 8, further comprising the steps of:
authenticating the domain owner, using a first authentication mechanism, for purposes of DNS record modification;
denying the requested modification to the at least one DNS record responsive to failure of the authentication using the first authentication mechanism;
authenticating the domain owner, using a second authentication mechanism that is different than the first authentication mechanism, for purposes of policy configuration; and
denying the configuration request responsive to failure of the authentication using the second authentication mechanism.
11. The method of claim 8, further comprising the steps of:

authenticating the domain owner, using a first authentication mechanism, for purposes of DNS record modification;

denying the requested modification to the at least one DNS record responsive to failure of the authentication using the first authentication mechanism;

authenticating the domain owner, using a second authentication mechanism that imposes a degree of inconvenience that is greater than another degree of inconvenience imposed by the first authentication mechanism, the second authentication mechanism used for purposes of policy configuration; and

denying the configuration request responsive to failure of the authentication using the second authentication mechanism.

12. The method of claim 7, wherein the at least one policy prohibits modifications of the at least one DNS record that point outside of infrastructure controlled by the domain owner.

13. The method of claim 7, further comprising the step of granting the requested modification conditional at least upon an IP address in the at least one DNS record being contained within at least one range specified by the policy.

14. The method of claim 7, further comprising the step of granting the requested modification conditional at least upon a name in the at least one DNS record being part of another domain also owned by the domain owner.

15. The method of claim 7, further comprising the step of granting the requested modification conditional at least upon a name in the at least one DNS record being within infrastructure controlled by the owner.

Claims

1. A non-transitory computer-readable medium embodying a program executable in a computing device, the program comprising:
 - code that authenticates a domain owner for purposes of domain name system (DNS) record modification using a first mechanism of authentication;
 - code that receives a request to modify at least one DNS record associated with a first domain owned by the domain owner;
 - code that validates the request by applying at least one policy to the request, the validation responsive to success of the authentication, the at least one policy prohibiting modifications of the DNS record that refer to an identifier that is outside of an infrastructure controlled by the domain owner while permitting modifications of the DNS record that is part of the first domain when the modified DNS record is part of a second domain also owned by the domain owner;
 - code that denies the request to modify the at least one DNS record responsive to failure of the validation;
 - code that authenticates the domain owner for purposes of policy configuration using a second mechanism of authentication for the domain owner, wherein the second mechanism of authentication for configuring the at least one policy is different than the first mechanism used for DNS record updates;
 - code that receives a request to configure the at least one policy; and
 - code that denies the request to configure responsive to failure of the authentication for purposes of policy configuration.

2. The computer-readable medium of claim 1, further comprising code that grants the request to configure responsive to success of the authentication.

3. The computer-readable medium of claim 1, wherein the code that validates determines that an IP address field is present in the at least one DNS record and successfully validates the request to modify conditional at least upon the address field being contained within one or more ranges specified by the at least one policy.

4. The computer-readable medium of claim 1, wherein the code that validates determines that a canonical name is present in the at least one DNS record and successfully validates the request to modify conditional at least upon the canonical name being on a whitelist specified by the at least one policy.

5. The computer-readable medium of claim 1, wherein the code that validates determines that an exchange domain name is present in the at least one DNS record and successfully validates the request to modify conditional upon the exchange domain name being within the infrastructure controlled by the domain owner.

6. A system, comprising:
at least one computing device; and
a domain name system (DNS) policy manager executable in the at least one computing device, the DNS policy manager comprising:

logic that validates request a request to modify a DNS record associated with a domain owned by a domain owner by applying at least one policy to the request, the validation responsive to success of authentication of the domain owner, the policy prohibiting modifications of the DNS record that point outside of an infrastructure controlled by the domain owner while permitting modifications of the DNS record that is part of the domain when the modified DNS record is part of a second domain also owned by the domain owner;

logic that selectively grants a requested modification to the at least one DNS record based at least upon an application of the at least one policy; and

logic that authenticates the domain owner for purposes of policy configuration using a different second mechanism of authentication for the domain owner.

7. The system of claim 6, the DNS policy manager further comprising logic that configures the at least one policy responsive to a configuration request by the domain owner.

8. The system of claim 6, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon an IP address in the at least one DNS record being contained within at least one range specified by the at least one policy.

9. The system of claim 6, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon a name in the at least one DNS record being part of another domain also owned by the domain owner.

10. The system of claim 6, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon a name in the at least one DNS record being within the infrastructure controlled by the owner.

11. The system of claim 6, wherein the logic that selectively grants the requested modification grants the requested modification conditional at least upon a name in the at least one DNS record being contained within a whitelist specified by the at least one policy.

12. A computer implemented method, comprising:
receiving, in a computing device, a request to modify at least one domain name system (DNS) record associated with a first domain owned by a domain owner;
comparing, via the computing device, the request to modify the at least one DNS record with at least one policy, the at least one policy prohibiting modifications of the at least one DNS record that point outside of an infrastructure controlled by the domain owner while permitting the request to modify the at least one DNS record that is part of the first domain when the modified at least one DNS record is part of a second domain

also owned by the domain owner, the at least one policy being configurable by the domain owner;

selectively granting, via the computing device, the requested modification to the at least one DNS record based at least upon the comparison; and

authenticating, via the computing device, the domain owner for purposes of policy configuration using a different second mechanism of authentication for the domain owner.

13. The computer implemented method of claim 12, further comprising:
configuring, via the computing device, the at least one policy responsive to a configuration request by the domain owner.

14. The computer implemented method of claim 13, further comprising:
authenticating, via the computing device, the domain owner for purposes of policy configuration; and
denying, via the computing device, the configuration request responsive to failure of the authentication.

15. The computer implemented method of claim 13, further comprising:
authenticating, via the computing device, the domain owner, using a first authentication mechanism, for purposes of DNS record modification;

denying, via the computing device, the requested modification to the at least one DNS record responsive to failure of the authentication using the first authentication mechanism;

authenticating, via the computing device, the domain owner, using a second authentication mechanism that is different than the first authentication mechanism, for purposes of policy configuration; and

denying, via the computing device, the configuration request responsive to failure of the authentication using the second authentication mechanism.

16. The computed implemented method of claim 13, further comprising:

authenticating, via the computing device, the domain owner, using a first authentication mechanism, for purposes of DNS record modification;

denying, via the computing device, the requested modification to the at least one DNS record responsive to failure of the authentication using the first authentication mechanism;

authenticating, via the computing device, the domain owner, using a second authentication mechanism, the second authentication mechanism being used for purposes of policy configuration; and

denying, via the computing device, the configuration request responsive to failure of the authentication using the second authentication mechanism.

17. The computer implemented method of claim 12, wherein the at least one policy prohibits modifications of the at least one DNS record that point outside of infrastructure controlled by the domain owner.

18. The method of claim 12, further comprising granting, via the computing device, the requested modification conditional at least upon an IP address in the at least one DNS record being contained within at least one range specified by the policy.

19. The method of claim 12, further comprising granting, via the computing device, the requested modification conditional at least upon a name in the at least one DNS record being within infrastructure controlled by the owner.

20. The method of claim 12, further comprising granting, via the computing device, the requested modification conditional at least upon a name in the at least one DNS record being contained within a whitelist specified by the policy.