

TS;DR (too spammy didn't read) – Challenges disclosing vulnerabilities to small and medium sized businesses

Anne Hennig, Sebastian Neef, Peter Mayer

Introduction

01

About myself

- **Anne Hennig**
  - M.A. in communication science / science communication
  - Since 2021 research associate / PhD candidate for research group Security – Usability – Society (SECUSO) @Karlsruhe Institute of Technology (KIT)
  - Topics:
    - Vulnerability notifications
    - Communication of security and privacy issues
    - Security awareness



Vulnerability Notifications – or “You have been hacked!”

- **Vulnerabilities** = misconfigurations or compromises
- **Vulnerability notifications** = messages to operators of vulnerable systems
  - Sender = those who find vulnerabilities
  - Recipient = owner of vulnerable system (e.g., website / domain owner)
  - Notification channel = direct (e-mail, phone, letter)
- **Vulnerability disclosure** = disclosing vulnerabilities to vendors
  - Sender = those who find vulnerabilities
  - Recipient = vendor of a system that has a vulnerability (e.g., WordPress)
  - Notification channel = “coordinated” (e.g., portal, bug bounty program, direct)

Fix it – if you can! Towards Understanding the Impact of Tool Support and Domain Owners' Reactions to SSHFP Misconfigurations

02

Link to paper: https://s.kit.edu/sshfp-paper

Background

- Notifcations have proven effective, yet remediation rates are low [2, 3, 6 - 11, 13]
- **Open question:** How to best support those affected?
  - Tool support is recommended by previous work [5, 9, 13, 15]
    - tool support significantly increased remediation where used
    - tool support helped to verify the legitimacy of a notification
  - Users find self-test tool helpful [7]
  - Tool support has not been proven effective [5, 9]
    - but high delivery failures, usability issues [9]
    - sender had a different affiliation than the institution hosting the tool [7]

Background

- Just because an issue is not remediated does not imply that affected individuals are not aware or careless [9]
- **Open question:** What are individual reasons for non-remediation and how do they affect remediation rates?
  - Lack of resources, complex coordination within a company, or lack of knowledge might hinder remediation processes [14]
  - Motivations and reactions might be different for misconfiguration issues [5, 12]

Research Questions

RQ1 Does an interactive self-test tool increase remediation compared to textual information?

RQ2 Does an interaction effect exist between the provider of the tool and the sender of the notification?

RQ3 What are the reasons for domain owners' non-remediation of the misconfiguration?

RQ4 How do domain owners react to notifications about misconfigurations?

Methodology – Notifications

- Notification text based on related work [13, 16]
- Six different notifications sent from KIT and TU Berlin
  - First e-mail: March 6, 2024
  - One reminder e-mail: March 26, 2024 (neither remediated nor responded)
- Periodic scans to measure remediation rate
- Analysis of email responses to measure reaction and reasons

```
Greeting {{firstname1}} {{lastname1}},

As part of a research project at {{UNI}}, we are identifying misconfigurations related to your
DNS infrastructure.

We have already contacted you about this on 06.03.2024.

With this message, we merely want to inform you about the behavior we have observed. If you have
already made changes to the SSHFP records, this message likely refers to unconfigured DNSSEC.

Whether you wish to take further action is up to your discretion. As part of our study, you will
not be at any disadvantage if you choose to do nothing further. After this reminder email, we
will not contact you again.

Do you think our email is a mistake? Or are you already aware of the problem? We would greatly
appreciate your feedback in a short reply to this email.

Otherwise, here is the information from our first email again:

# What is the issue?
You are using SSHFP DNS records on the following domains to utilize DNS-based HostKey
verification for SSH:

{{subdomain_1}}
{{subdomain_2}}
{{subdomain_3}}
{{subdomain_4}}

In the course of our investigation, we have found that the entries you have set are not
correctly configured. There are two possible scenarios:

1) The HostKey fingerprints in the SSHFP DNS records do not match the actual HostKeys or HostKey
fingerprints of the SSH server.

2) The SSHFP DNS records are not being securely transmitted because DNSSEC is not configured.

# What can happen?

For scenario 1: If the HostKey fingerprints in the DNS and the corresponding SSH server do not
match, the HostKey verification cannot be automatically performed by the SSH program. This means
that the SSH program (e.g., OpenSSH) will prompt the user for manual verification. Manual
verification carries the risk that it may be done incorrectly or not at all.

For scenario 2: DNS is a plaintext protocol that, without DNSSEC, does not provide guarantees
for the authenticity of the transmitted data. The SSHFP standard requires that these DNS records
be securely transmitted (e.g., via DNSSEC). If this is not the case, network-based attackers can
manipulate or remove the transmitted SSHFP records. This means that automated HostKey
verification will fail or may accept manipulated HostKeys from the attacker.

In both scenarios, this could potentially lead to attackers gaining access to your SSH
credentials and thus to your infrastructure.

You can verify the configuration we identified using a self-test tool. There you will also find
more information on how to proceed. To use the tool, enter {{link}} in your browser and then
verify yourself with the token {{token}}. You can also use the direct link: {{link}}?t={{token}}

We recommend that you resolve the issue. You can consult your IT administrator or DNS hosting
provider on how to set the configuration correctly.

Best regards,
{{Sender}}

--

{{Sender's footer}}
```

Greeting {{firstname1}} {{lastname1}},

As part of a research project at {{UNI}}, we are identifying misconfigurations related to your DNS infrastructure.

We have already contacted you about this on 06.03.2024.

With this message, we merely want to inform you about the behavior we have observed. If you have already made changes to the SSHFP records, this message likely refers to unconfigured DNSSEC.

Whether you wish to take further action is up to your discretion. As part of our study, you will not be at any disadvantage if you choose to do nothing further. After this reminder email, we will not contact you again.

Do you think our email is a mistake? Or are you already aware of the problem? We would greatly appreciate your feedback in a short reply to this email.

Otherwise, here is the information from our first email again:

What is the issue?
You are using SSHFP DNS records on the following domains to utilize DNS-based HostKey verification for SSH:

{{subdomain_1}}
{{subdomain_2}}
{{subdomain_3}}
{{subdomain_4}}

In the course of our investigation, we have found that the entries you have set are not correctly configured. There are two possible scenarios:

1) The HostKey fingerprints in the SSHFP DNS records do not match the actual HostKeys or HostKey fingerprints of the SSH server.

2) The SSHFP DNS records are not being securely transmitted because DNSSEC is not configured.

personalized salutation

motivation

blue text:
reminder notification

description of the issue

```
# What can happen?

For scenario 1: If the HostKey fingerprints in the DNS and the corresponding SSH server do not
match, the HostKey verification cannot be automatically performed by the SSH program. This means
that the SSH program (e.g., OpenSSH) will prompt the user for manual verification. Manual
verification carries the risk that it may be done incorrectly or not at all.

For scenario 2: DNS is a plaintext protocol that, without DNSSEC, does not provide guarantees
for the authenticity of the transmitted data. The SSHFP standard requires that these DNS records
be securely transmitted (e.g., via DNSSEC). If this is not the case, network-based attackers can
manipulate or remove the transmitted SSHFP records. This means that automated HostKey
verification will fail or may accept manipulated HostKeys from the attacker.

In both scenarios, this could potentially lead to attackers gaining access to your SSH
credentials and thus to your infrastructure.

You can verify the configuration we identified using a self-test tool. There you will also find
more information on how to proceed. To use the tool, enter {{link}} in your browser and then
verify yourself with the token {{token}}. You can also use the direct link: {{link}}?t={{token}}

We recommend that you resolve the issue. You can consult your IT administrator or DNS hosting
provider on how to set the configuration correctly.

Best regards,
{{Sender}}

--

{{Sender's footer}}
```

threat model

Additional information and possibility to verify in link groups

possibilities to contact and verify the sender

Summary

- We measured
  - whether an **interactive self-test tool** increases remediation (RQ1)
    - ➢ Results: sig. differences between text only KIT and tool different TU Berlin
  - whether **interaction effects** exist between the sender of the notification and the institution hosting the tool (RQ2),
    - ➢ Results: no interaction effects found
  - why domain owners **do not remediate** the misconfiguration (RQ3),
    - ➢ Results: not an issue, no option to remediate
  - and **how they respond** to our notification (RQ4).
    - ➢ Results: mostly friendly, but also disagreement and annoyance

“I believe it‘s incredible difficult to fight against this flood of spam“: Towards Enhancing Strategies for Creating Effective Vulnerability Notifications

03

Link to paper: https://s.kit.edu/hacking-paper

Background

- Notifcations have proven effective, yet remediation rates are low [2, 3, 6 - 11, 13]
- **Open question:** Which sender is most suitable?
  - Related work showed mixed results wrt sender
    - sender has no impact on remediation rate [6, 8, 11, 17, 19, 20]
    - legal sender is most effective with respect to remediation [5]
    - Recipients state sender is important to assess the trustworthiness of a notification [5, 6]

Background

- **Open question:** Which effect do sanctions have?
  - Related work has proposed incentives (i.e., consequences) [5, 9, 10, 17, 18]
    - technical incentives (quarantining network connections) has proven effective [10, 17]
    - legal incentives (fines) can significantly increase remediation [5]
    - only applicable in certain circumstances
    - maybe dependent on sender? [5, 12]
- **Open question:** Why do those affected not remediate?
  - Lack of resources, complex coordination within a company, or lack of knowledge might hinder remediation processes [14]

Research Questions

RQ1 Which framing has what impact on the remediation of compromised websites?

RQ2 Which sender has what impact on the remediation of compromised websites?

RQ3 Can we identify an interaction effect between sender and framing wrt the remediation of compromised websites?

RQ4 What are reasons for website owners to not remediate their websites even after being notified twice?

Methodology – Notifications

- Notification text based on pre-study interviews [16]
- Three senders: Federal CERT, hosting provider, university
- Three framings: technical, reputational, neutral
  - Consecutive notifications between April ’22 and Nov ’23
  - One reminder e-mail each after two weeks
- Periodic scans to measure remediation rate
- Phone calls after 8 weeks

To: <recipient.email>

From: <sender>

Subject: Important information on your website <domain>

<title> <lastname>,

We are contacting you with important information about your website <domain>.

Within a research project we currently analyze search engine entries and detected several subpages which redirect to fraudulent online shops. It looks like your website was manipulated by third parties.

You can easily reproduce it when you search in your browser for “site:<source.fqdn> <hacking_keyword>”. The search results show all entries to your website that are known to the search engine. You can see that some entries do not match the content of your website. If you clicked on those links, you would be redirected to a fraudulent online shop.

We recommend you to restore the security of your website. Please verify our information and solve the problem as soon as possible. You can find further information at https://www.web-inspection.de/faq.

<framing>

Best regards,
<sender>

———————————

<signature>

To: <recipient.email>

From: <sender>

Subject: Important information on your website <domain>

<title> <lastname>,

We are contacting you with important information about your website <domain>.

Within a research project we currently analyze search engine entries and detected several subpages which redirect to fraudulent online shops. It looks like your website was manipulated by third parties.

You can easily reproduce it when you search in your browser for "site:<source.fqdn> <hacking_keyword>". The search results show all entries to your website that are known to the search engine. You can see that some entries do not match the content of your website. If you clicked on those links, you would be redirected to a fraudulent online shop.

We recommend you to restore the security of your website. Please verify our information and solve the problem as soon as possible. You can find further information at https://www.web-inspection.de/faq.

<framing>

Best regards,
<sender>
———————————
<signature>

personalized salutation

motivation

verification of the issue

further information

consequences

possibilities to contact and verify the sender

Framings

- **<neutral>:** without framing
- **<technical-generic>:** Please check this issue. If the problem is not remediated, we will have to report your case to your hosting provider. They can block your webspace or the affected files in your webspace.
- **<technical-hoster1>:** Please check this issue and let us know what you have done. Please note that if there is no response or if the problem persists, we may be forced to block your webspace or the affected files in your webspace on <date>
- **<technical-hoster2>:** Please check this and let us know what action you have taken. Please note that if there is no response or if the problem persists, we will be forced to take further action.

Framings

- **<reputation-generic>:** Please check this issue. Please note that you may suffer reputational damage if you do not remediate the problem. This can be, for example, block listings with security providers or warning messages from the browser, so that your website is indexed as a security risk for outsiders.
- **<reputation-CERT>:** Please check this issue and let us know what you have done. Please note that various web reputation services assess the credibility of websites according to a scoring procedure, which may also include issues such as this one. Users of such web reputation services may therefore receive a warning, or their access may be blocked completely.

Summary

- We measured
  - what effect **different framings** have on the remediation of compromised websites (RQ2),
    - ➢ Results: no significant differences between different framings
  - what effect **different senders** have on the remediation of compromised websites (RQ1)
    - ➢ Results: significant difference towards control group, not between different senders
  - if an **interaction effect** exist between sender and framing (RQ3)
    - ➢ Results: no interaction effect
  - why domain owners **do not remediate** the misconfiguration (RQ4),
    - ➢ Results: website owners were not aware of notification (spam)

Discussion

04

What are your experiences?

- Have you ever found a vulnerability?
- Have you ever disclosed a vulnerability you found?
  - If so: How? What are your experiences?
  - If not: Why?
- In your opinion:
  - What are the most important factors for vulnerability notifications?
  - What needs to be improved?
  - What are possible research questions for related work?

Potential Future Work

05

Open Questions

1. Effect of tool support needs further investigation
   - Tool provider and sender from different domains?
2. Additional strategies needed to increase awareness – enhancing background knowledge?
3. Incentives that can arise fear not recommended – encouraging framings?
4. …

References

06

References

[1] S. Neef and N. Wisiol, “Oh SSH-it, What’s My Fingerprint? A Large-Scale Analysis of SSH Host Key Fingerprint Verification Records in the DNS,” in International Conference on Cryptology and Network Security. Springer, 2022, pp. 71–88.

[2] F. Li, G. Ho, E. Kuan, Y. Niu, L. Ballard, K. Thomas, E. Bursztein, and V. Paxson, “Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension,” in Proceedings of the 25th International Conference on World Wide Web, ser. WWW ’16. Montreal, Quebec, Canada: International World Wide Web Conferences Steering Committee, 2016, pp. 1009–1019. [Online]. Available: https://doi.org/10.1145/2872427.2883039

[3] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson, “You’ve Got Vulnerability: Exploring Effective Vulnerability Notifications,” in 25th USENIX Security Symposium (USENIX Security 16), 2016, pp. 1033–1050. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/li

[4] M. Maass, M.-P. Clement, and M. Hollick, “Snail Mail Beats Email Any Day: On Effective Operator Security Notifications in the Internet,” in 16th International Conference on Availability, Reliability and Security (ARES 2021). Vienna, Austria: ACM, New York, NY, USA, 2021, pp. 1–13.

[5] M. Maass, A. Stöver, H. Pridöhl, S. Bretthauer, D. Herrmann, M. Hollick, and I. Spiecker, “Effective notification campaigns on the web: A matter of Trust, Framing, and Support,” in 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, 2021, pp. 2489–2506. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/maass

[6] B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow, “Didn’t You Hear Me? - Towards More Successful Web Vulnerability Notifications,” in Proceedings of the 25th Annual Symposium on Network and Distributed System Security (NDSS ’18), 2018, pp. 1 – 15. [Online]. Available: https://swag.cispa.saarland/papers/stock2018notification.pdf

[7] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, “Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification,” in 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, 2016, pp. 1015–1032. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/stock

References

[8] E. Zeng, F. Li, E. Stark, A. P. Felt, and P. Tabriz, “Fixing HTTPS Misconfigurations at Scale: An Experiment with Security Notifications,” in The 2019 Workshop on the Economics of Information Security (2019), Boston, MA, 2019, pp. 1 – 19. [Online]. Available: https://www.semanticscholar.org/paper/Fixing-HTTPS-Misconfigurations-at-Scale%3A-An-with-Zeng-Li/b22c522c6201f8545e1626deaf6ca43db52444d7

[9] F. O. Çetin, C. H. Gañán, M. T. Korczynski, and M. J. G. v. Eeten, “Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning,” ser. 16th Workshop on the Economics of Information Security (WEIS 2017), San Diego, 2017, pp. 1–23. [Online]. Available: http://resolver.tudelft.nl/uuid:621f4a4f-e5d9-4f04-abc4-46252f9db3db

[10] O. Çetin, C. Gañán, L. Altena, S. Tajalizadehkhoob, and M. v. Eeten, “Tell Me You Fixed It: Evaluating Vulnerability Notifications via Quarantine Network,” 2019 IEEE European Symposium on Security and Privacy (EuroS&P), vol. 00, pp. 326–339, 2019.

[11] O. Çetin, M. H. Jhaveri, C. Gañán, M. v. Eeten, and T. Moore, “Understanding the role of sender reputation in abuse reporting and cleanup,” Journal of Cybersecurity, vol. 2, no. 1, pp. 83–98, 2016. [Online]. Available: https://academic.oup.com/cybersecurity/article/2/1/83/2629556

[12] C. Utz, M. Michels, M. Degeling, N. Marnau, and B. Stock, “Comparing Large-Scale Privacy and Security Notifications,” Proceedings on Privacy Enhancing Technologies, vol. 2023, no. 3, p. 173–193, 2023

[13] M. Maaß, H. Pridöhl, D. Herrmann, and M. Hollick, “Best Practices for Notification Studies for Security and Privacy Issues on the Internet,” in 16th International Conference on Availability, Reliability and Security, ser. The 16th International Conference on Availability, Reliability and Security. Vienna, Austria: Association for Computing Machinery, 2021, pp. 1–10.

[14] A. Stöver, N. Gerber, H. Pridöhl, M. Maass, S. Bretthauer, I. S. genannt Döhmann, M. Hollick, and D. Herrmann, “How Website Owners Face Privacy Issues: Thematic Analysis of Responses from a Covert Notification Study Reveals Diverse Circumstances and Challenges,” Proc. Priv. Enhancing Technol., vol. 2023, pp. 251–264, 2023. [Online]. Available: https://petsymposium.org/popets/2023/popets-2023-0051.php

References

[15] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey, and J. A. Halderman, “The Matter of Heartbleed,” in Proceedings of the 2014 Conference on Internet Measurement Conference, IMC ’14, ser. IMC ’14. Vancouver, BC, Canada: Association for Computing Machinery, 2014, pp. 475–488. [Online]. Available: https://doi.org/10.1145/2663716.2663755

[16] A. Hennig, F. Neusser, A. A. Pawelek, D. Herrmann, and P. Mayer, “Standing out among the daily spam: How to catch website owners’ attention by means of vulnerability notifications,” in Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems, ser. CHI EA ’22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3491101.3519847

[17] Çetin, O., Gañán, C., Altena, L., Kasama, T., Inoue, D., Tamiya, K., Tie, Y., Yoshioka, K., and van Eeten, M., “Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai,” in Proceedings of the Network and Distributed System Security Symposium, 2019. [Online]. Available: https://www.ndss-symposium.org/ndss-paper/cleaning-up-the-internet-of-evil-things-real-world-evidence-on-isp-and-consumer-efforts-to-remove-mirai/

[18] Vasek, M., and Moore, T., “Do Malware Reports Expedite Cleanup? An Experimental Study”, In 5th Workshop on Cyber Security Experimentation and Test, CSET ’12, Bellevue, WA, USA, August 6, 2012. USENIX Association, 1 – 8. https://www.usenix.org/conference/cset12/workshop-program/presentation/vasek

[19] Rodríguez, E., Verstegen, S., Noroozian, A., Inoue, D., Kasama, T, van Eeten, M., and Gañán, C., “User compliance and remediation success after IoT malware notifications”, Journal of Cybersecurity 7, 1 (07 2021), [Online]. Available: https://doi.org/10.1093/cybsec/tyab015

[20] Çetin, O., Altena, L., Gañán, C., and van Eeten, M., “Let Me Out! Evaluating the Effectiveness of Quarantining Compromised Users in Walled Gardens”, In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). USENIX Association, Baltimore, MD, 251–263. https://www.usenix.org/conference/soups2018/presentation/cetin