Peer review: An Overview of DNS Cache Poisoning

SUMMARY

The paper gives an introduction to the Domain Name System and how it is exploitable with DNS Poisoning. It is used to direct a user to a compromised server. To achieve the poisoning of the DNS entry, there are various different ways. These ways are all stated and explained in the paper. It also gives insight into the found solutions to the vulnerability. The most important solution is called DNSSEC is explained in detail.

STRENGTH

+ The paper gives a good overview of the DNS poison attack scheme.
+ It lists offensive and defensive measurements.
+ It shows that there is still work needed in adapting the defensive measurements.
+ There is a common thread in the explanation of the attacks.

WEAKNESS

- There are no real examples in the paper, it only lists the different attack strategies.
- The abstract lacks some motivation.
- There is no conclusion in the abstract.
- The paper is explaining how to flush your DNS on Windows.
- The predicting random number generation part is lacking an introductory part.
- There are often abbreviations used without an explanation.
- There is no Related Work
- There is no Background provided despite probably needed to explain the DNS System.
- There is no Discussion.
- There is no Evaluation.
- There is no Conclusion.
- There is no structure in the paper it is just a concatenation of Headings.
- There are no Threat Models explained in different attack strategies, suddenly there is system access.
- The malware part is a repetition of the bruteforce part.

COMMENTS

- The introduction is a good introduction to the Domain Name System, which could be moved into a background
- While explaining the DNS a figure would be good to understand the structure better
- In general more detail would be nice, how does a DNS package look like in contrast to a poisoned one.
- Make it more clear how DNS request is intercepted, and an attacker knows there is one being sent.
- Explain the ”birthday paradox”
- Explain the UDP protocol and in the same procedure the TCP protocol. This would fit into a background.
- In the last paragraph of the first DNS poison attack you fail to explain why all future responses will be ignored.
- Clearly describe your attacks, what does an attacker know what abilities do he has. Do not introduce the compromised servers’ step by step.
- Explain TTL more, again in the Background for DNS.
- For the explanation of DNSSEC a figure could be helpful, as there are suddenly a lot of different new Keys introduced.
- At the start of the last paragraph to DNSSEC list the tasks needed to implement DNSSEC
- At the end of the last paragraph to DNSSEC list the attacks that come with partial deployment of DNSSEC. Make a chapter from these attacks.
- In the bruteforce part, there is 32-bit field used but not explained.
- In the end of the first paragraph of bruteforce ”when” is often used. Make the Threat model more clear
- In the example of the bruteforce paragraph there seems to be logical error: We already have access to the target and need it to visit a malicious website to execute code on the target.
- The predicting the random generator seems to be a side-channel attack, which is not clearly stated.
- Make the threat model of the random number generator attack more clear.
- In the malware part, there is a focus on Windows. There are other operating systems out there.
- Evaluate the current state of DNS make a conclusion if the attacks are still feasible.
- More drawn out examples would be helpful to understand the topic more easily.
- When do we know that a victim has sent a DNS request?