A novel zone walking protection for secure DNS Server

Arnob Paul, Md. Hasanul Islam, Md. Shohrab Hossain

Bangladesh University of Engineering and Technology, Bangladesh

& Husnu S. Narman,

Marshall University, Huntington, WV, USA

Presentation at

World Telecommunication Symposium

April 22-24, Washington, DC, USA

Outline

- DNS and DNSSEC
- Zone-walking attack
- NSEC and NSEC3
- Our proposed approach
- Experimental evaluation
- Results
- Conclusion

DNS Protocol History

- Comes in 1983, more than 35 years ago from now
- Used for mapping between domain name and IP address
- https://something.example.com → 1.2.3.4

Advantages of DNS

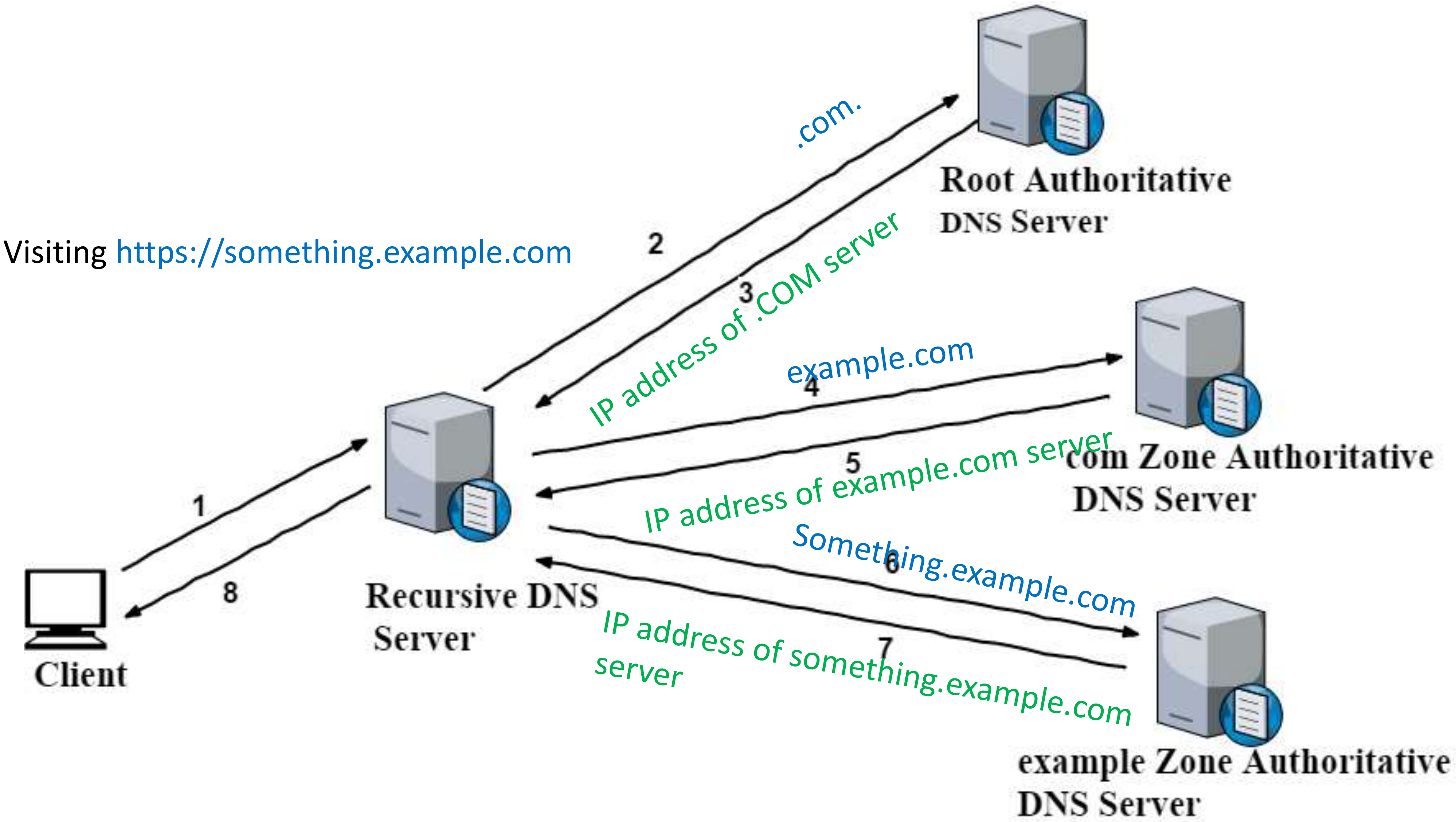
- Highly scalable, so still used even now
- Makes it easy for human so that IP address need not to be memorized
- Acts as a phonebook

Disadvantages of DNS

- Not designed for DNS data integrity
- Not designed in mind of data authenticity
- Highly vulnerable to DNS cache poisoning attack

Outline of DNS

Visiting https://something.example.com



From DNS to DNSSEC

- Each individual DNS query response comes with a signature
- Also ensures proof of no record (via NSEC or NSEC3)

Drawbacks of DNSSEC

- Enabling DNSSEC may expose obscured zone content
- Some DNS servers worry about ‘zone walking’
- NSEC3 was developed to eliminate ‘zone walking’ but it is costly in terms of performance
- More vulnerable to DDoS attack

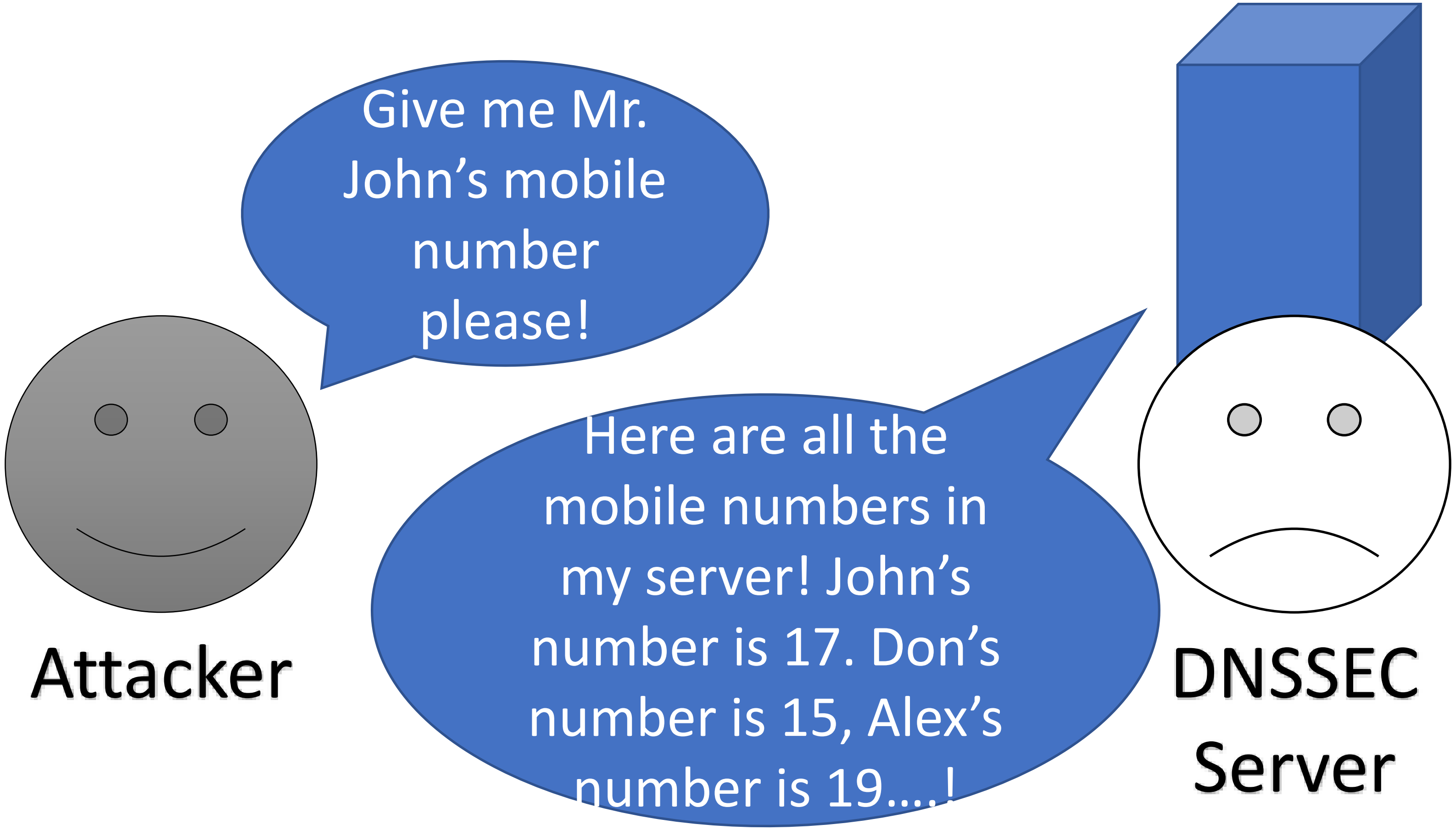
Current Condition

- DNSSEC applied in Root level nameservers
- As of 2016, 89% of top level domains (TLDs) zones signed.
- DNSSEC is more available for domains by CloudFlare

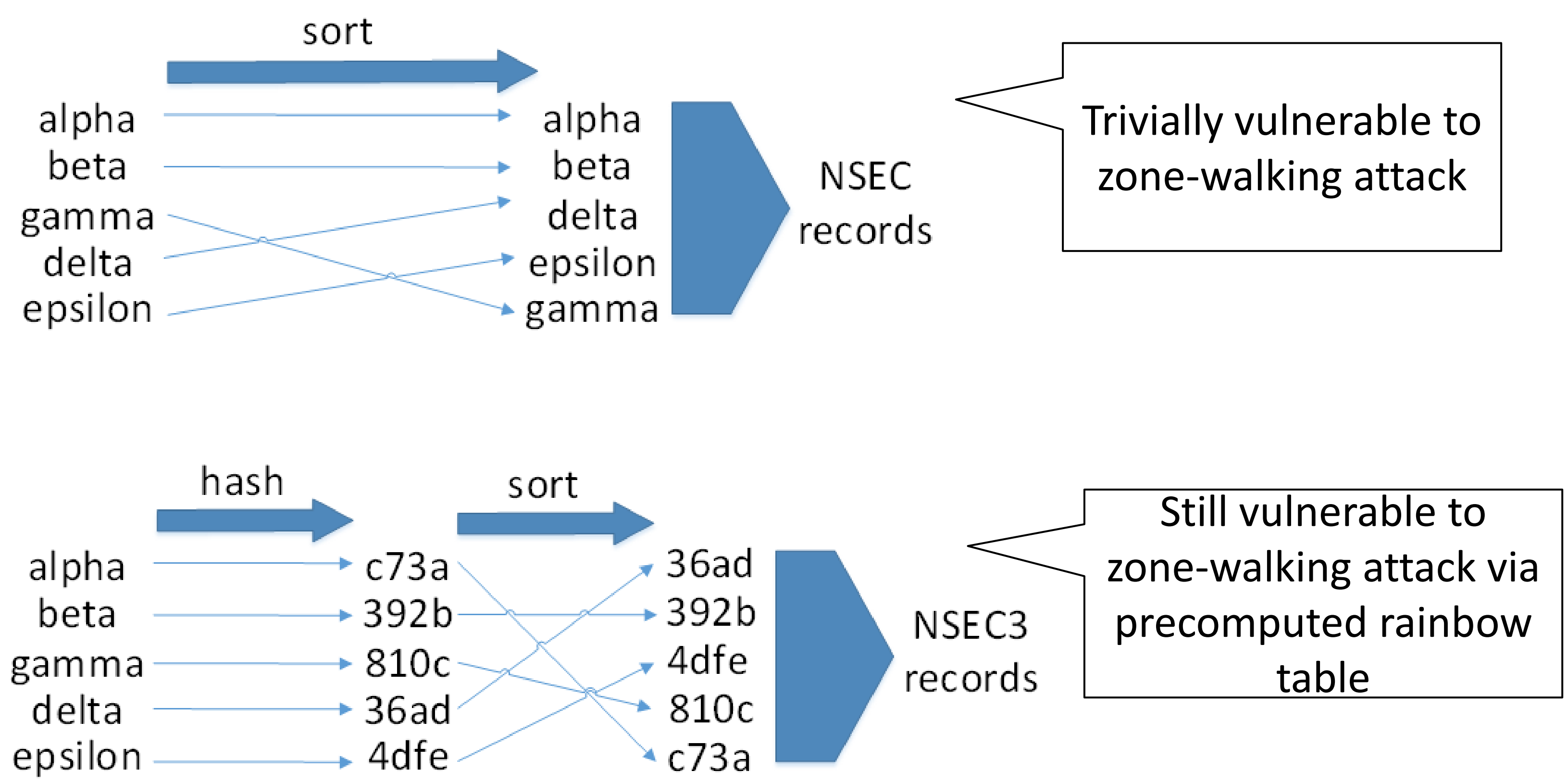
Zone Walking Attack

Attack overview

- Retrieve all DNSSEC server data at once



NSEC vs NSEC3



Our Contribution

- **Dividing list:** Instead of proving the next record name in the zone like NSEC, another nonexistent name is provided.
- **Low profiling:** Client requests are profiled to identify
- zone walking attackers.

Novelty

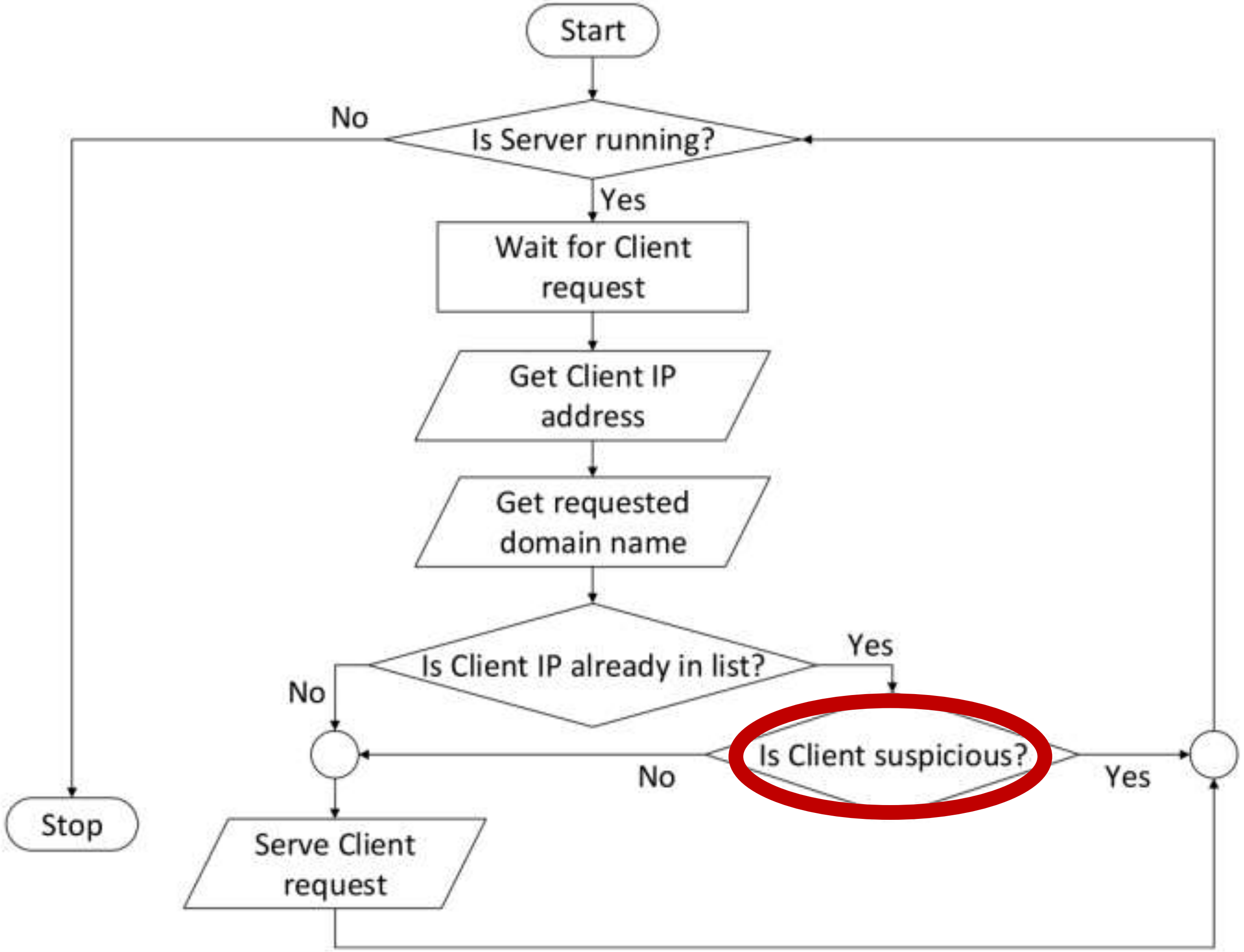
- Alternative approach to zone walking attack which does not use hashing

Low Profiling

- Detect suspicious client behaviour
- Block probable attacker

Hey suspicious attacker! Get out of my server!

Low Profiling Algorithm Flow Chart



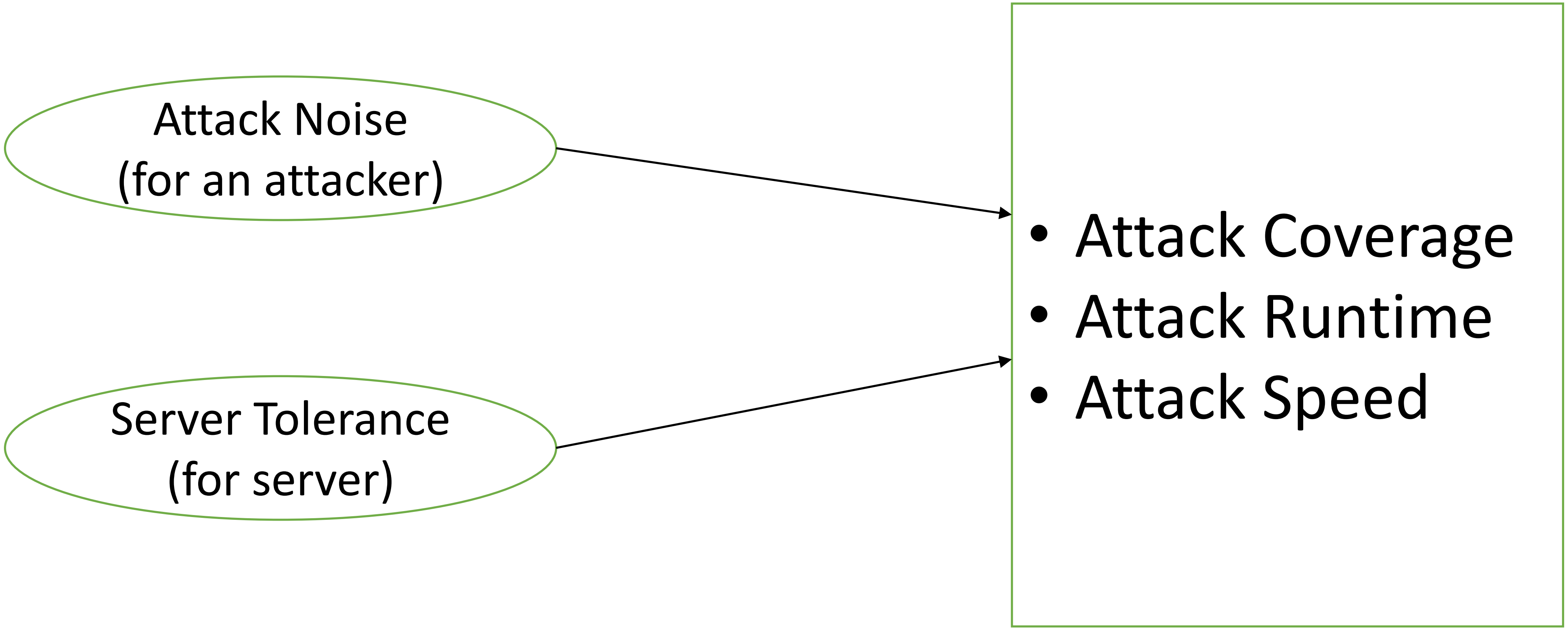
Implementation

- Detect if the domain names are in alphabetical order

```java
public boolean isSuspicious(String domain) {
    long currentTime = System.currentTimeMillis();

    // check if already suspicious activity found and within block time period
    if (isSuspicious && ((currentTime - blockTime) < suspiciousClientBlockTimeElapsed)) return true;

    // clear suspicious status
    isSuspicious = false;

    // cleanup old request records
    cleanupOldRecords();

    // check if suspicious
    if (!requestRecords.isEmpty()) {
        Record lastRecord = requestRecords.getLast();

        // check if requested domain breaks lexicographical order (not suspicious)
        if (lastRecord.domain.compareTo(domain) >= 0) {
            requestRecords.clear();
        }
        // check if previous requests in lexicographical order exceeds the constant (suspicious)
        else if (requestRecords.size() >= totalSuspiciousRecordsForEachClient) {
            isSuspicious = true;
            requestRecords.removeFirst();
        }
    }

    // add domain request to activity record
    Record record = new Record(domain);
    requestRecords.add(record);

    // assign blockTime (if suspicious) and return result
    blockTime = currentTime;
    return isSuspicious;
}
```

https://github.com/arnobpl/DNSSEC/blob/master/src/DNSSEC/ServerPack/Security/LowProfiling.java

Evaluation of Proposed Low Profiling Algorithm

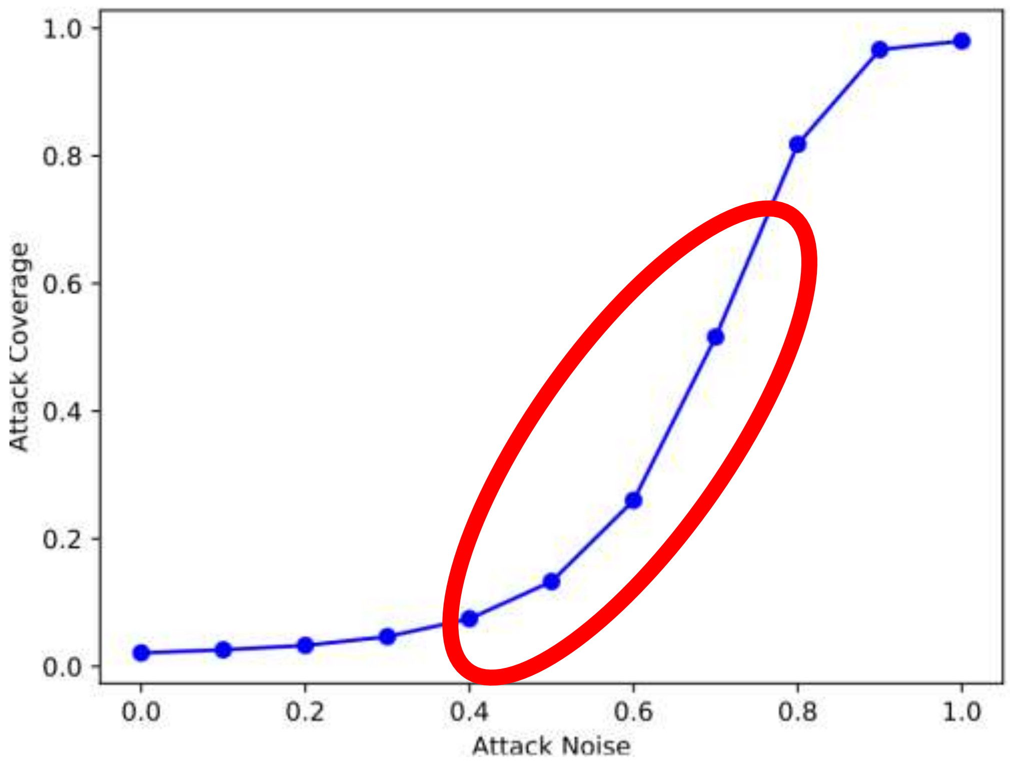


Parameters of our Evaluation

- **Attack Noise:** Attack Noise is the probability of breaking alphabetical order of domain query to server.
- **Server Tolerance:** Server Tolerance (the number of suspicious records) is the number of continuous requests received alphabetically from a client needed by DNSSEC server to identify the client as an attacker.
- **Attack Coverage:** The ratio between the number of domains fetched by the attacker and the number of domains stored in the server.
- **Attack Runtime:** The elapsed runtime of the attacker client (in milliseconds).
- **Attack Speed:** The speed of fetching domain by the attacker (in the number of domains fetched per millisecond).

Evaluation of Low Profiling (cont.)

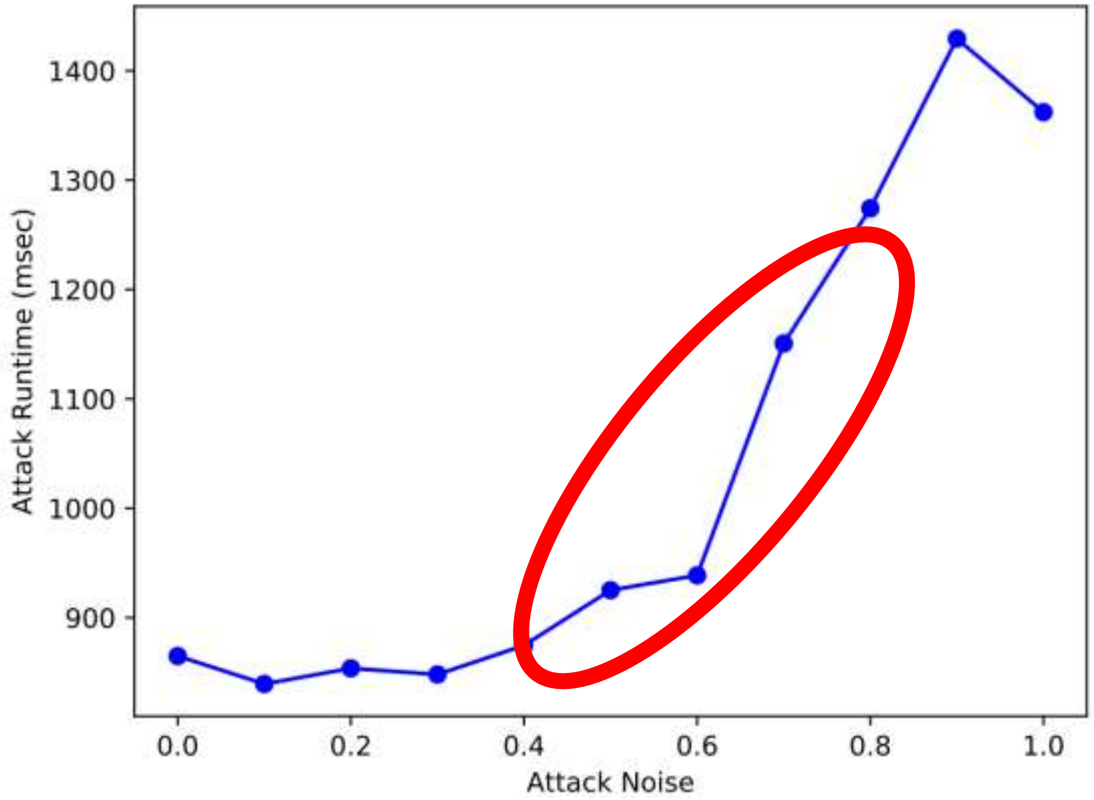
- If the probability of breaking alphabetical order of requested domains by an attacker is low, then the DNSSEC server can easily identify that attacker after ten subsequent requests.



Attacker-side evaluation

Evaluation of Low Profiling (cont.)

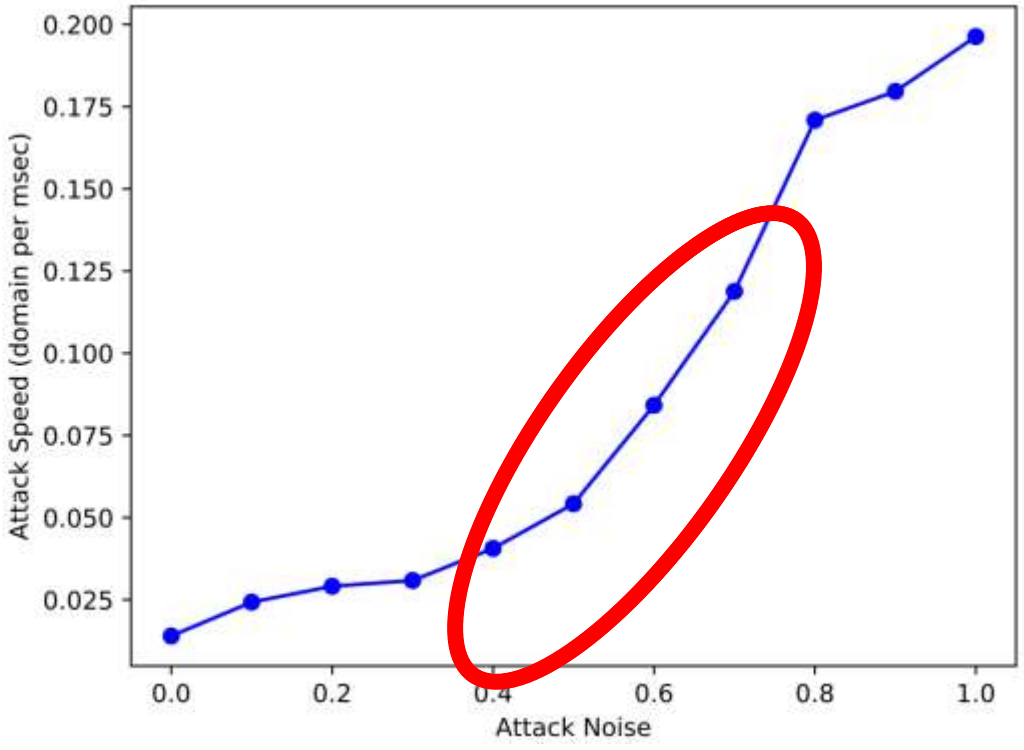
- The runtime of attack increases almost linearly for every noise level of attack.
- As attack noise increases, the attacker will be able to retrieve more domains from the server.



Attacker-side evaluation

Evaluation of Low Profiling (cont.)

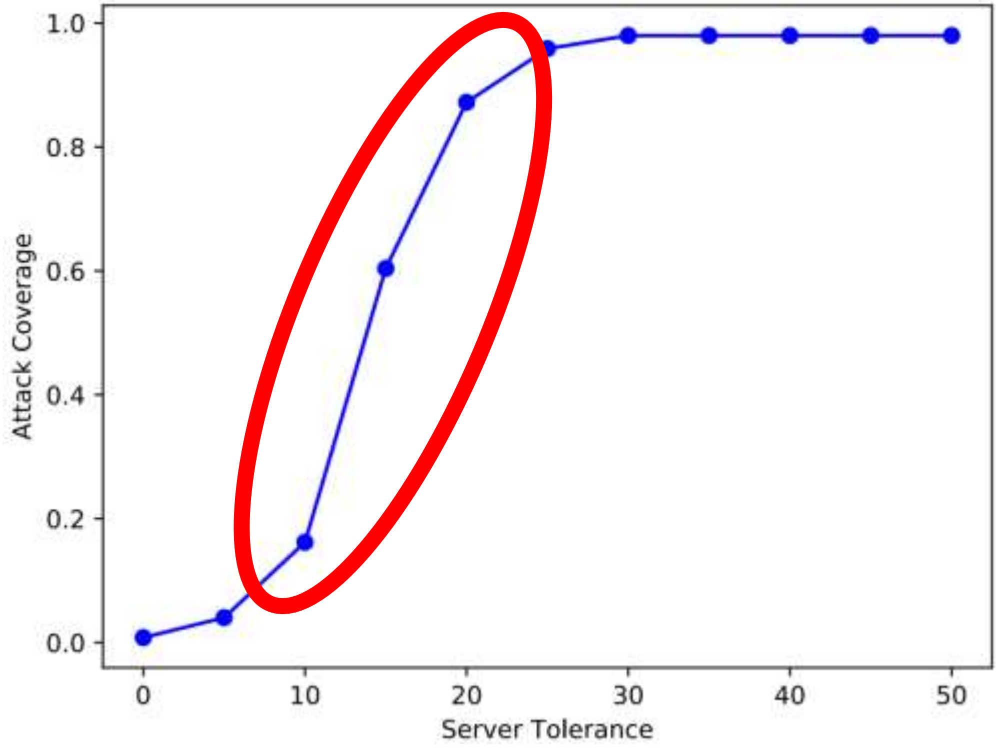
- Domain retrieved per millisecond increases slowly as noise increases for attacker.



Attacker-side evaluation

Evaluation of Low Profiling (cont.)

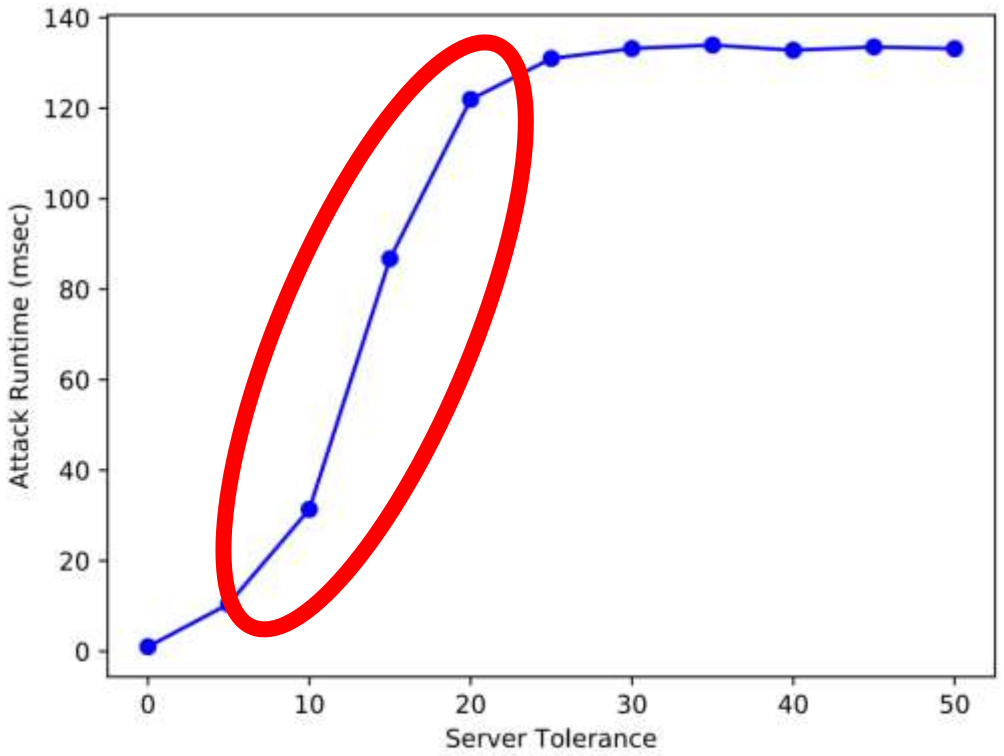
- As Server Tolerance (i.e., the number of suspicious records needed to identify an attacker) increases, the domains fetched by an attacker from DNSSEC server increases proportionately up to some total suspicious records.



Server-side evaluation

Evaluation of Low Profiling (cont.)

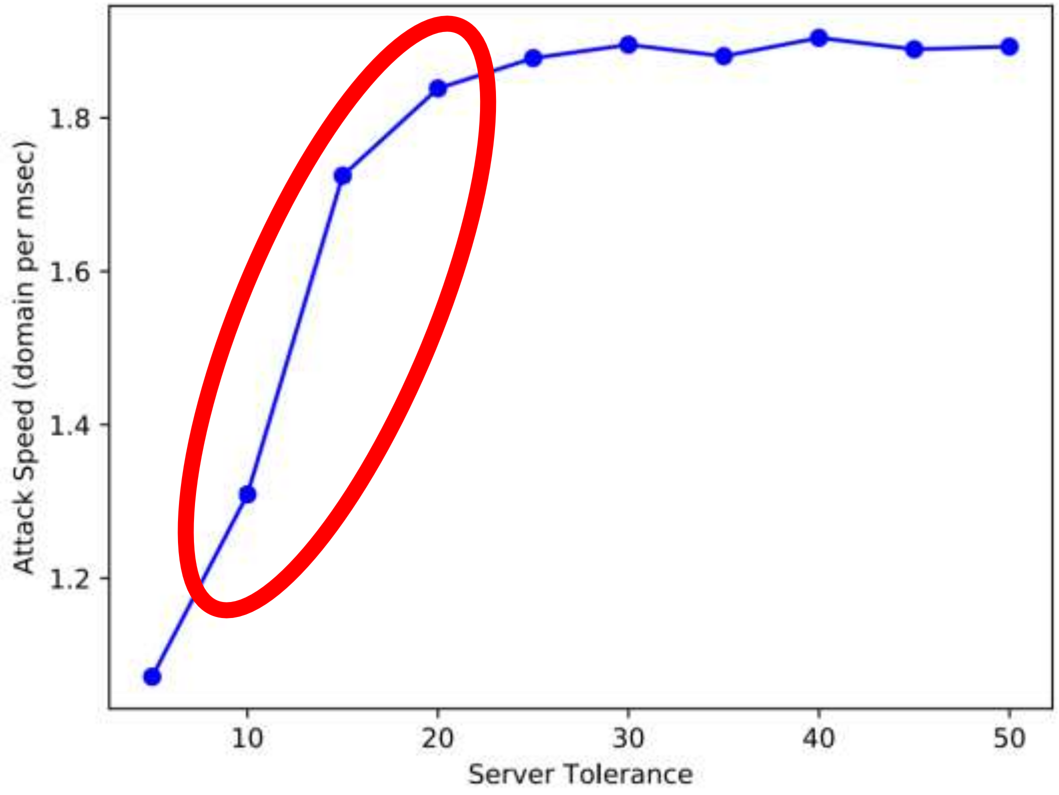
- As Server Tolerance increases, the attacker runtime will increase proportionally.



Server-side evaluation

Evaluation of Low Profiling (cont.)

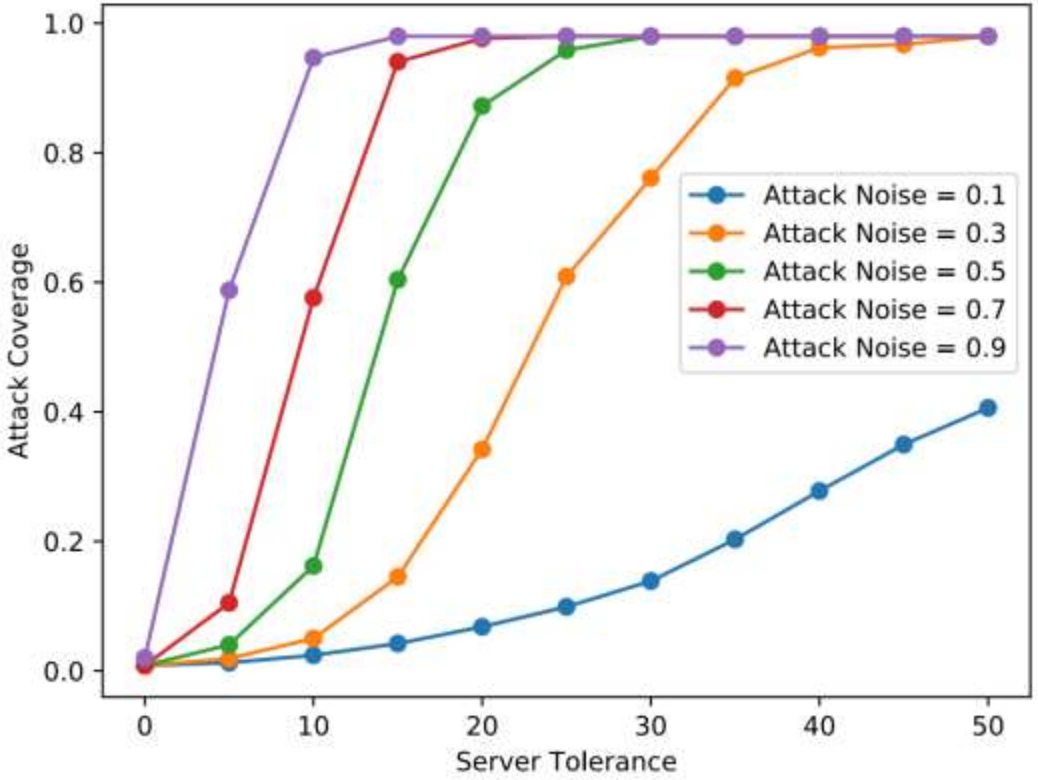
- <u>Attack speed (domains per msec)</u> slowly increases because of the increase of the rate of domain received is more than the increase of the runtime of attack.



Server-side evaluation

Evaluation of Low Profiling (cont.)

- Higher attack noise means a stronger attacker who can fetch more domains even with limited server tolerance.
- Weaker attack (with attack noise of 0.1) cannot fetch all the domains even with a high value of server tolerance.



Conclusion

- Zone walking attack attempts to get all existing domain information from a secured DNS server.
- Although the NSEC3 protocol was proposed to defend against zone walking attack, it takes much time to protect against such an attack.
- In this paper, we have proposed and implemented a defense mechanism (low profiling) against zone walking attack to mitigate the intensity of such an attack.
- We have presented our results for different performance metrics.

Thank you!