CryptoWatch

Analyzing the Diversity of Cryptographic Algorithms of Internet-Connected Services

Stud Ent - *sten42@hs-esslingen.de* - University of Esslingen

Supervisors: Prof. Dr. Tobias Heer, Nils Lohmiller {tobias.heer, nils.lohmiller}@hs-esslingen.de

ESSLINGEN UNIVERSITY

IT Security & Data Analysis

1. Motivation: State of Cryptography

Internet-connected services use different cryptographic **algorithms** and **key lengths** to secure their communication. Services that implement TLS use **certificates**. Over time, these certificates, algorithms, and key lengths change. For example, since 2020, browsers require a shorter certificate validity period of at most one year. Cryptographic algorithms will be replaced if more efficient ones become available or if those become insecure. Services that use asymmetric algorithms are threatened by quantum computers. Therefore, **Post-Quantum Cryptography (PQC)** emerges to protect these systems in the future.

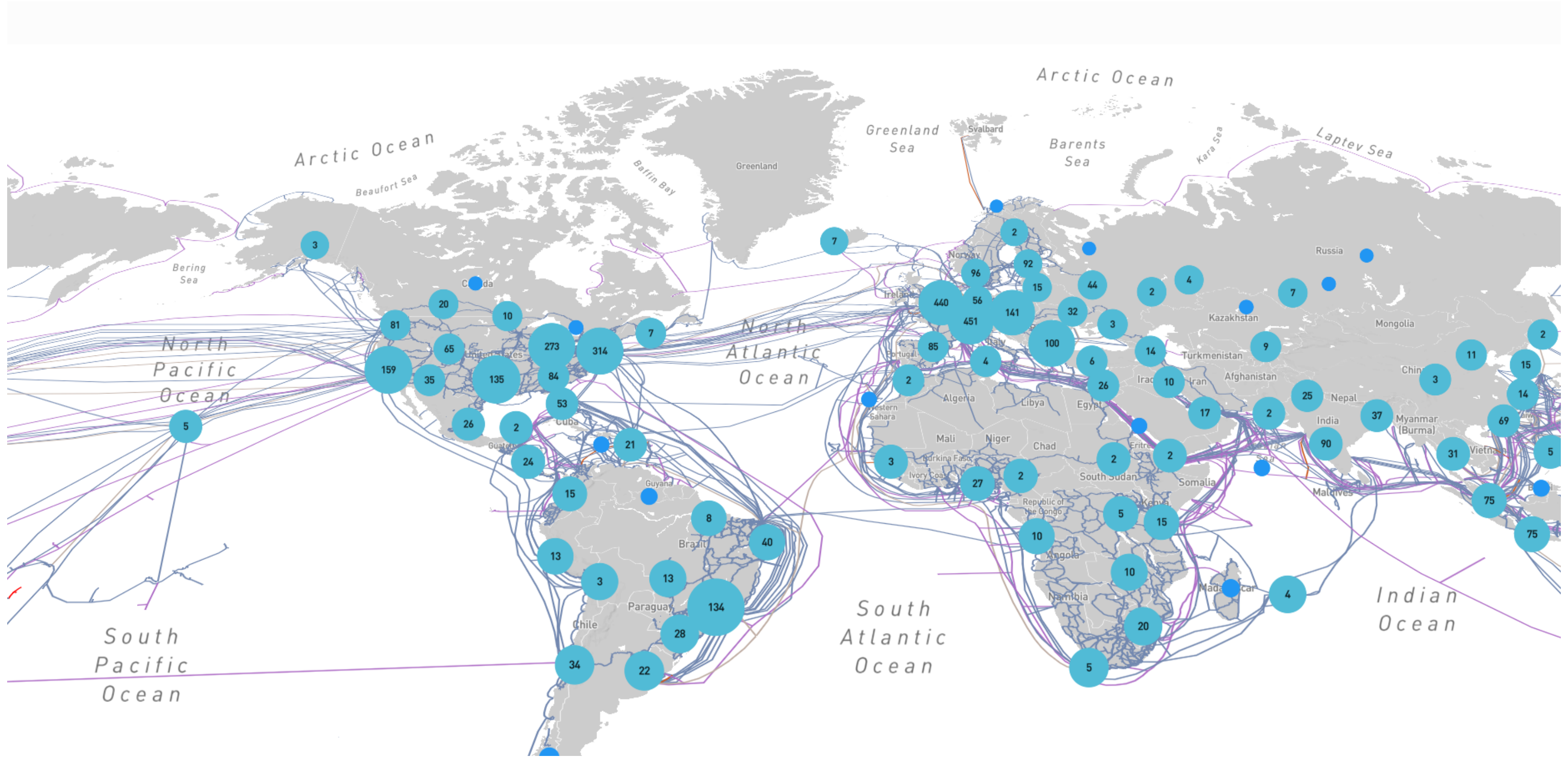

Figure 1: Internet Infrastructure Visualization [1]

However, not only will systems need to be protected in the future, current systems already need protection mechanisms. One possible attack scenario is ***save now decrypt later***. In this scenario, an attacker stores asymmetrically encrypted data and assumes that he can decrypt it with the help of quantum computers in the future. Such attacks can only be prevented by considering which algorithms will still be secure in the future. A transition of all asymmetric algorithms to pure PQC or a combination of PQC and classical asymmetric cryptography takes time. The sooner the transition to PQC begins, the better [3].

2. Research Idea: How do Cryptographic Algorithms Change over Time?

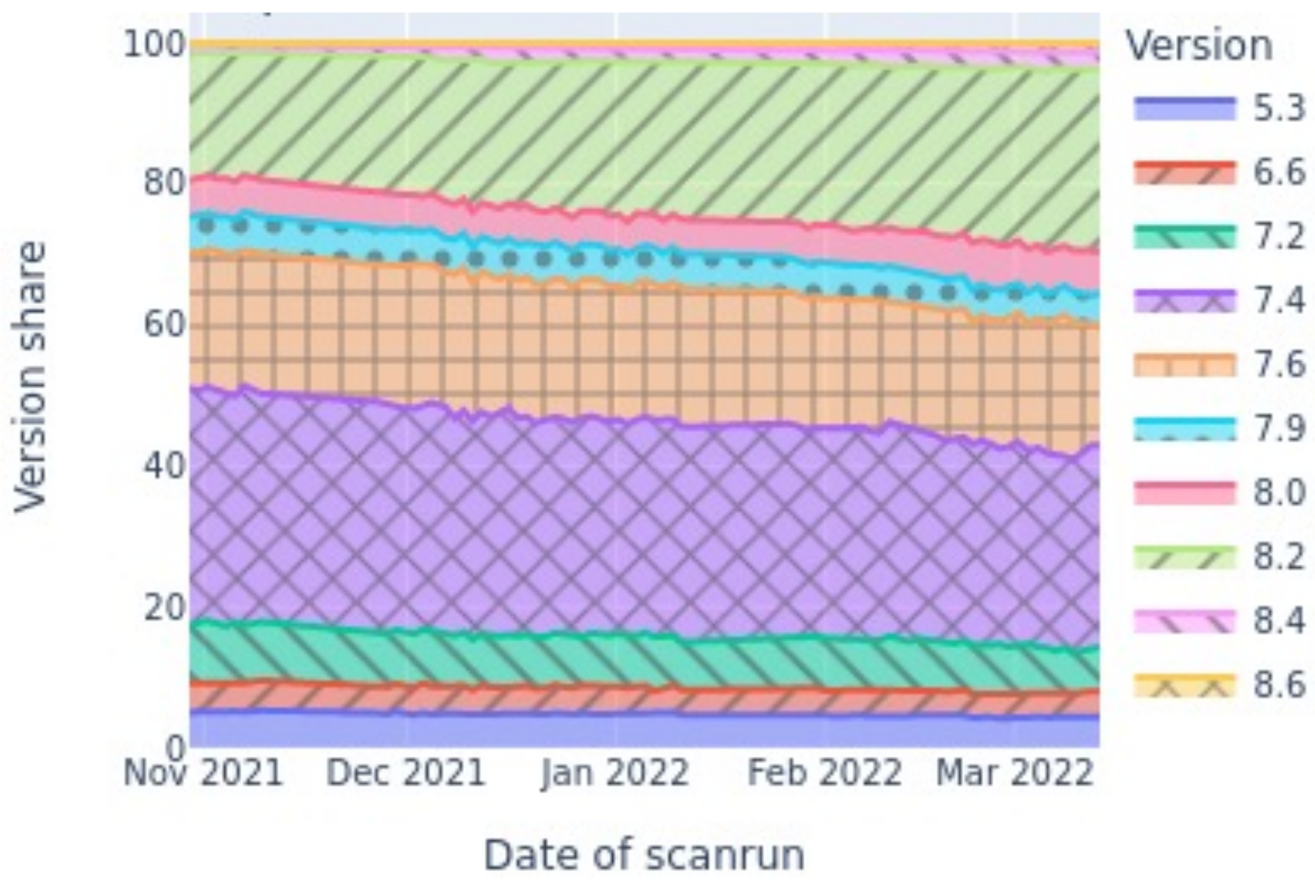

Figure 2: OpenSSH versions change over time, along with them different cryptographic algorithms are used

- Due to the reduced validity period of the certificates, they have to be renewed more frequently
- We will investigate whether the **algorithms change during the renewal of certificates**
- Are there any **regional differences/inconsistencies**?
- Figure 2 shows how OpenSSH versions change over time. We will do the same but for certificates and cryptographic algorithms.
- The transition towards PQC poses new challenges
- Google and Cloudflare have shown the practical use of hybrid PQC and asymmetric cryptography [2].
- We examine whether there are Internet services that *already support PQC algorithms*

3. Key Research Challenges

- What should a **scanning pipeline** look like?
- What is the **current state** of cryptographic algorithms?
  - Which cryptographic algorithms are commonly used?
  - Which key lengths are often used?
  - Have PQC algorithms already been implemented?
- What changes after **certificate renewals**?
- Are there regional differences?

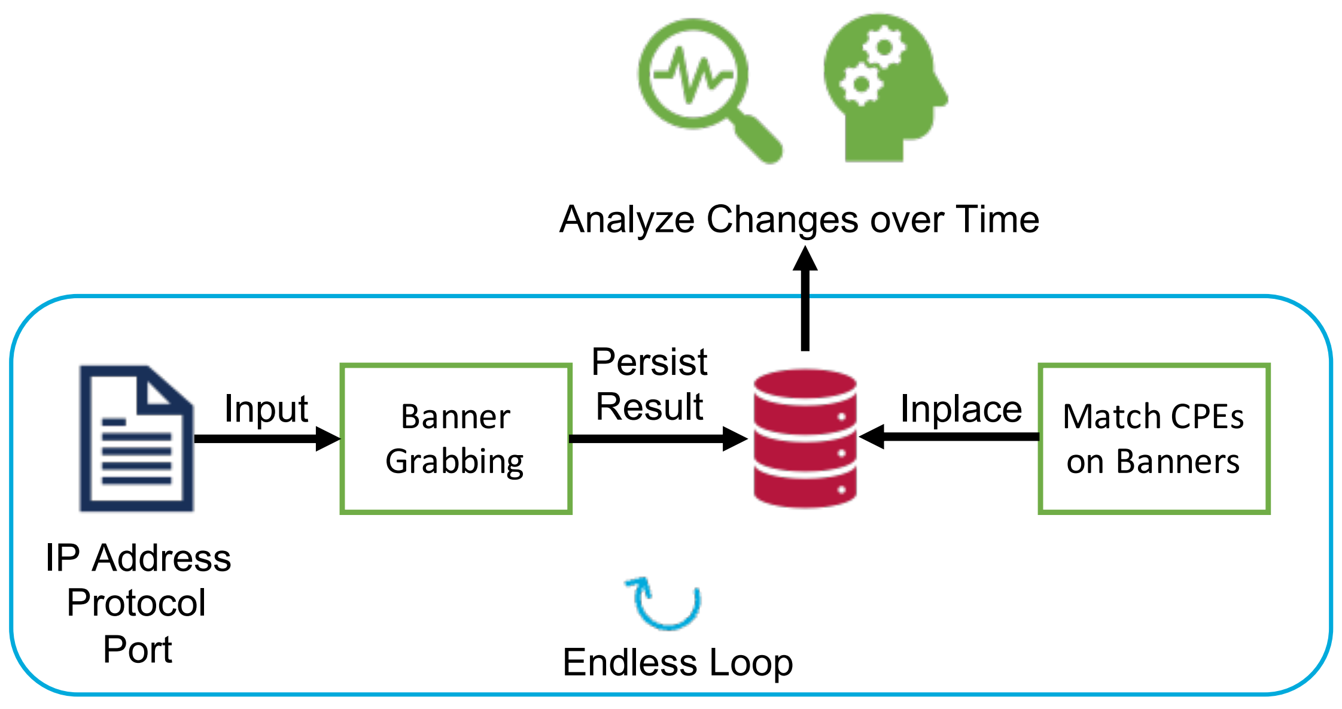

Figure 3: Scanning Pipeline

4. References

[1] Infrapedia, [Online]. Available: https://www.infrapedia.com/img/infrapedia_map.bd515ab6.png (visited on 09/18/2023).

[2] K. Kwiatkowski and L. Valenta, "The tls post-quantum experiment", (Oct. 30, 2019), [Online]. Available: https://blog.cloudflare.com/the-tls-post-quantum-experiment/.

[3] D. Ott, C. Peikert, *et al.*, "Identifying research challenges in post quantum cryptography migration and cryptographic agility", *arXiv preprint arXiv:1909.07353*, 2019.