Passive SSH Key Compromise via Lattices

Keegan Ryan, **Kaiwen (Kevin) He**, George Arnold Sullivan, Nadia Heninger

Paper
ia.cr/2023/1711

Summary

We recovered **189 SSH keys** by **passively** observing **real internet traffic**.

To do so, we developed an **efficient** lattice-based attack that exploits **naturally miscomputed signatures**.

There is a **simple** and **effective** way to **mitigate** this attack: verify the signature is correct before sending it out.

Faulty Signatures

Potential sources of faulty signatures are

Corrupted Storage | Software Bugs | Faulty hardware

Impact

Once the SSH host key is compromised, an attacker can

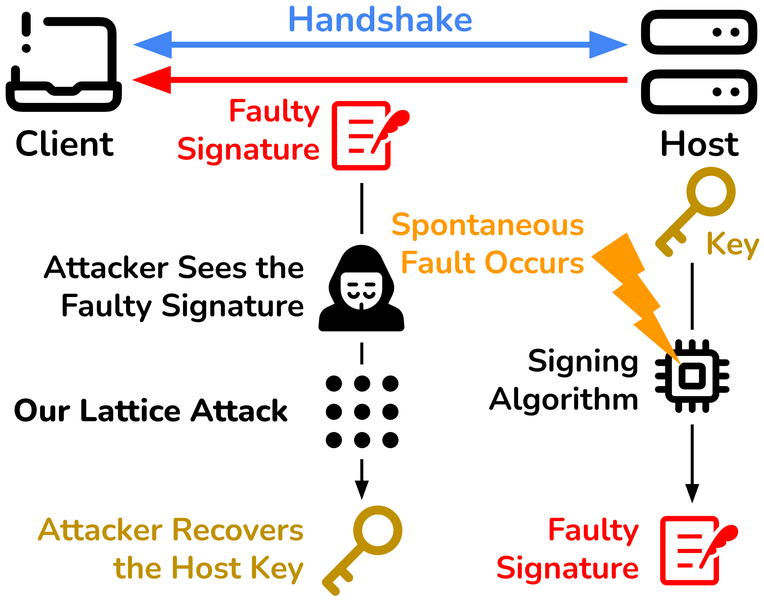
Intercept Passwords | Impersonate the Host | Inject Commands

Therefore, vulnerable hosts should **rotate keys** after mitigating this attack.

Our Attack

Our lattice-based attack allows a **passive eavesdropper** to recover the host key from a **single** faulty signature **under 0.2 seconds** for most cipher suites.

A passive attack is possible because in the SSH protocol, **the signature is sent in plaintext**.



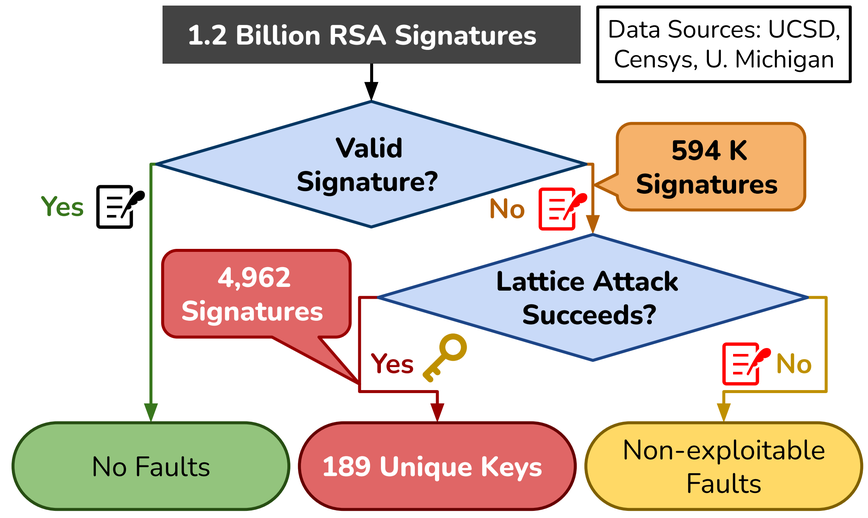
Advantages

Prior works have explored signature fault attacks on SSH that require *active* connections to hosts, which are *expensive* and *detectable*.

Passive attacks are **stealthier** and scales to **larger amounts of internet traffic**.

Evaluation

We collected and analyzed **1.2 billion signatures** from university network taps and Zmap scans



Response

Since we recovered keys from real world devices, we **responsibly disclosed** our research to their vendors: Cisco, Zyxel, Hillstone Networks, and Mocana. Many **investigated promptly** and **provided mitigations**.

We also considered notifying operators of vulnerable devices, but decided it would be infeasible due to the difficulty of identifying operators from our data.