

Forum:[Hack Forums](#)

Thread: [Sniffing private keys via mitm](#)

jinovas - March 30, 2016, 8:33 am

Hey this is my first post and found lots of good reads on here and love learning and reading about new stuff and how things are done. This especially helps at my job since I'm the most knowledgeable in security on my team.

I did have a question, however, on private RSA keys. I am able to easily log the private keys when a certain chromium store app is connected to its servers to decrypt the network traffic via wireshark and adding a simple sslkeylog environment variable in windows 8.1 and windows 10. But this so far I've tested on the host computer. I remember in the past, doing this via mitm, having issues and having some success(if I remember correctly); but it was so long ago and I don't remember what I did to reproduce it. But, I was hoping someone might be able to help clarify if this can also be done via mitm or have a way to grab those private keys via mitm? Or if anyone had any thoughts on it?

I've googled around and haven't had too much success so far researching how private RSA keys are handled or obtained from passive sniffing.

Thanks! ?