Back to School: On the (In)Security of Academic VPNs

Ka Lok Wu [1] Man Hong Hue [1,2] Ngai Man Poon [1]
Kin Man Leung [3] Wai Yin Po [1] Kin Ting Wong [1] Sze Ho Hui [1]
Sze Yiu Chau [1]

[1]Department of Information Engineering, The Chinese University of Hong Kong

[2]Georgia Institute of Technology

[3]The University of British Columbia

Aug 11, 2023

Motivation

- The Use of VPN to access internal services in organizations increases due to the pandemic
- Enterprise credentials, often being reused as Single Sign-On (SSO) credentials, are targets for **Initial Access Brokers** (IABs)
- We studied the category of VPNs that are used by organizations to provide remote access of the enterprise network to their employees: organizational VPNs
- Since it is difficult to obtain information of organizational VPNs, we focused on VPNs used by *academic institutions*, which tend to release their instructions for using the VPNs publicly online: **academic VPNs**
- To the best of our knowledge, this is the first comprehensive review of academic VPNs

Server Authentication

Three aspects that can go wrong in a VPN setup:

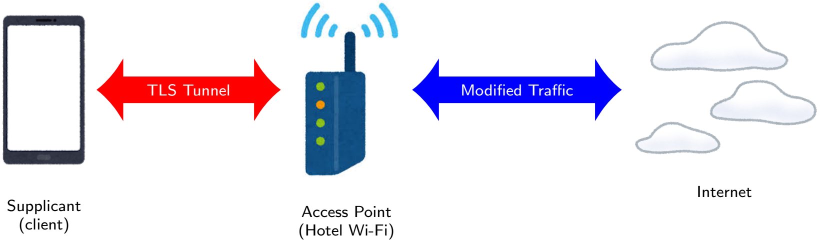
1. design and implementation of VPN front-ends
2. client-side configurations
3. back-end configurations

Methodology

1. We collected a list of 2097 publicly-available VPN instructions from a list of 6600 academic institutions
2. We manually reviewed the instructions to discover different VPN applications and protocols that are being used
3. We inspected the setup guides to see if they provide secure instructions
4. We tested 132 (front-end) VPN applications on 4 major OSs from 30 vendors to see if they implement certificate validation
5. We probed 2000 VPN gateways discovered from the setup guides to understand the back-end configurations

Man-in-the-Middle

- We consider the man-in-the-middle attacker model
- Active on-path attacker
- Can observe, modify and redirect network traffic
- e.g.:
  - When a user connects through a Wi-Fi, the network admin has full control over the traffic
  - Internet Service Provider (ISP), government authorities



Findings

Out of the 2097 setup guides,

- 149 (7.1%) use IPSec-PSK VPNs. Among them, 118 have PSKs publicly exposed
- 44 (2.1%) make use of PPTP VPNs. We inspected 19 of them and found that none of them provide server authentication at all

In both cases, an attacker can impersonate as the VPN server and perform credential theft.

TLS-based VPNs

- 94.4% (1981) of the setup guides prescribe the use of “TLS-based” VPNs
- We find basically all these apps use TLS to authenticate the server and exchange credentials inside the tunnel, e.g.:
  - One app uses TLS to authenticate and exchange a pre-shared key, and then uses the key to establish an IPSec tunnel for VPN
  - OpenVPN-based VPNs may use TLS to obtain a profile containing the security settings, then use OpenVPN protocol to establish a VPN tunnel
- If the server authentcation is not done properly here, then credential theft with MitM is possible

TLS MitM Test Cases

We used the open-source MitM tools *mitmproxy* and *SSLProxy* for testing.

We consider two test cases where the attacker replaces the server's certificate with:

1. a self-signed certificate with the same subject name and subject alternative names (SAN)
2. a certificate purchased from a commercial CA, but the domain name is different from the server's

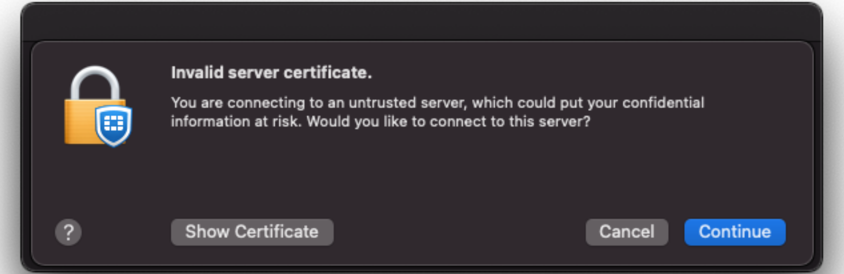
Findings

Out of the 132 VPN apps (160 if different “modes” are included) from 30 vendors, 56 distinct apps from 15 vendors automatically accepts untrusted server certificate **without user interaction**, with 2 apps accepting any certificates from commercial CAs.

For these applications, our MitM attack succeeds in obtaining credentials.

Findings (Cont'd)

- 70 apps, when seeing untrusted certificate, will *prompt* the user to accept (or reject) the certificate. Out of the 70,
  - 19 have the option to turn off certificate checking all together (no prompting)
  - 5 disable certificate checking by default



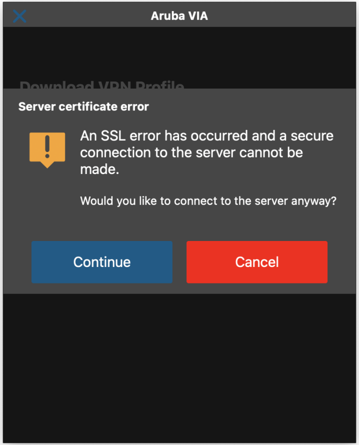
Invalid server certificate.

You are connecting to an untrusted server, which could put your confidential information at risk. Would you like to connect to this server?

Findings (Cont'd)

23 of the 70 apps do not show *sufficient information* for the user to determine if the certificate is valid. For example,

- the *SHA-256 fingerprint* of a certificate is sufficient
- only the *subject name* and *issuer name* are not sufficient since these are not authenticated



Server certificate error

An SSL error has occurred and a secure connection to the server cannot be made.

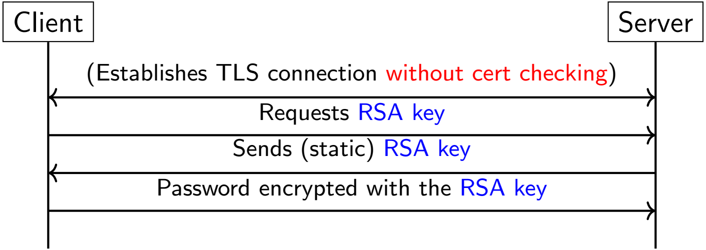
Would you like to connect to the server anyway?

Observation

We observed that some TLS apps would, instead of doing proper certificate validation, introduce **additional scrambling of the password** before sending it to the server.

Case Study: Sangfor EasyConnect

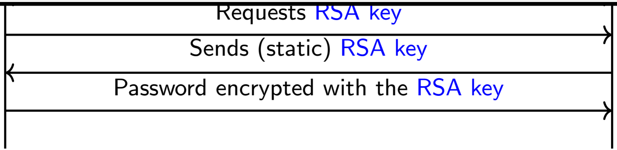
One interesting case of implementing ad-hoc security instead of proper cert validation: the program "secures" the password like this:


Client
Server
(Establishes TLS connection without cert checking)
Requests RSA key
Sends (static) RSA key
Password encrypted with the RSA key

Case Study: Sangfor EasyConnect

One interesting case of implementing ad-hoc security instead of proper cert validation: the program "secures" the password like this:

Since the RSA key is not authenticated, the attacker can simply replace the RSA key with its own, and obtain the password. We managed to set the public exponent to 1 and directly obtain the password.



RCE Attacks from Updates

- In addition to credential theft, we found 10 VPN apps vulnerable to remote code execution (RCE) attacks
- Those update requests made to the server do not have certificate validation
- Some application check the signature of the update executable, but some only check that the signing certificate is *from a commercial CA*, without checking the *subject name* or public key
  - By signing the executable with a code-signing certificate we bought under our name, we can bypass the certificate + signature check

Setup Guides for TLS-based VPNs

The crawled setup guides are then categorized into 4 categories:

1. `Unknown` when the instruction for the particular OS is *not found*
2. `Insecure` is due to the admins instructing the user to *turn off* certificate validation, or accept *any* certificate when prompted
3. `User Insecure` is where the user is not instructed to do anything, so the security depends on user behavior
4. `Secure` if the guide leads to either programmatic or manual rejection of untrusted certificates

Findings

We generated 6210 entries for all the academic units, OSs and apps considered. Excluding the `Unknown` entries (53.8%), `User Insecure` (24.4%) is the most common outcome observed. Luckily, `Insecure` instructions only account for 2.7% among all the outcomes.

Findings

We generated 6210 entries for all the academic units, OSs and apps considered. Excluding the `Unknown` entries (53.8%), `User Insecure` (24.4%) is the most common outcome observed. Luckily, `Insecure` instructions only account for 2.7% among all the outcomes.

Some IT admins only consider the *benign* case of connection but do not consider **exception handling**.

Credential theft is still possible if the attacker targets institutions with `Insecure` or `User Insecure` setup guides.

Back-end Configurations - TLS Vulnerabilities

- We curated a list of VPN server gateways from the setup guides
- We perform a scan using the open-source tool `TLS-Scanner` to look for existing TLS vulnerabilities, and also cross-checked their exploitability, which heavily depends on
  - the chosen ciphersuite, especially when the VPN client-server pairs are tightly-coupled
- Details can be found in the paper

Back-end Configurations - Classic Weakness of IKEv1

For IPSec PSK, IKEv1 aggressive mode are observed in 25 backends, which allows a passive MitM to perform offline dictionary attacks to recover the PSK.

Back-end Configurations - Server Certificates

We also analyzed the certificates obtained from the gateways.

- Out of the 1547 unique leaf certificates, 61 (3.9%) are expired
- 434 (28.1%) have chain that fail to verify
- Correlating the result back to the instructions, 40.7% of the gateways of `Insecure` setup guides have a certificate chain that can verify. Thus, it is inexcusable to prescribe `Insecure` setup guides.

Disclosure

We responsibly disclosed the vulnerabilities to the vendors and the setup guide issues to the academic institutions. However,

- The response rate from academic institutions is quite low
- Most vendors have confirmed the issues, only some of them have issued CVE IDs
- 2 vendors, in particular, confirmed the issues but refused to fix it. One of the vendors, Sangfor, claimed that (translated from Chinese):
  "We don't think this is a vulnerabilty. MITM hijack and traffic manipulation is a generic attack known to the community, and we will not fix this problem."

Conclusion

- We have presented a comprehensive review of academic VPNs, and found numerous implementation flaws in the application and the configuration issues
- Findings suggest many academic VPNs are easy targets for initial access brokers (IABs)

- For developers, proper server authentication should be enforced
- For IT admins, consider exceptional cases in preparing setup guides for users, and properly deploy secure configurations in the back-end

Thank you!

Questions?

For other questions, please contact {klwu@link, sychau@ie}.cuhk.edu.hk