Secure Systems Group, Aalto University

Thanh Bui, Siddharth Rao, Markku Antikainen, Tuomas Aura

Client-side Vulnerabilities in Commercial VPNs

Commercial VPNs

- Enhance security & privacy by tunnelling network traffic through a trusted remote server before forwarding it to the final destination
- **Our goal: Study how popular VPN providers setup, or instruct users to setup, their VPN clients**

Adversary model

- **Network attacker**: Anyone who can intercept and modify network traffic (e.g. rogue hotspot operator)
- **Local attacker**: Non-privileged user or process on the same computer (e.g. colleagues)

Our study

- 15 popular commercial VPN services
- 7 VPN protocols: PPTP, SSTP, L2TP/IPsec, Cisco IPsec, IKEv2, OpenVPN, SoftEther VPN
- Various vulnerabilities in the client configurations of all of the protocols

Results

Attacker	Protocol	Platform	# Vulnerable / # Supported	Vulnerability Description
Network	PPTP	W	10 / 12	Encryption is not enforced
	SSTP	U	3 / 3	Certificate verification failures are ignored
	L2TP/IPsec	W, M, U	13 / 13	Known preshared keys are used to setup IPsec tunnel
	Cisco IPsec	W, M, U	7 / 7	Known preshared keys are used to setup IPsec tunnel
	IKEv2	U	3 / 3	Client accepts any certified server certificate regardless of its identity
	SoftEther VPN	W, M	5 / 5	Server certificate is not verified
	Fallback strategy	W, M	2 / 5	Weak protocols are used as fallback options
Local	OpenVPN	W	6 / 13	Improper access control to user credentials
	SoftEther VPN	W, M	1 / 1	Unprotected management interface

(W: Windows, U: Ubuntu, M: macOS)