USENIX SECURITY 2022

Security at the End of the Tunnel

The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context

Veroniek Binkhorst, Tobias Fiebig, Katharina Krombholz, Wolter Pieters, and **Katsiaryna Labunets**
[k.labunets@uu.nl]

Problem Motivation

- VPN is one of the popular security and privacy measures on the Internet
- The end-users' perspective is well covered by recent empirical research[1]
- Increased VPN usage due to work-from-home orders during the COVID-19 pandemic
  - During the lockdown in March'20, VPN traffic increased by 200% vs February'20[2]
- Highly sensitive and confidential data flowing through the corporate VPNs
- Corporate users' perspective on VPN usage is neglected

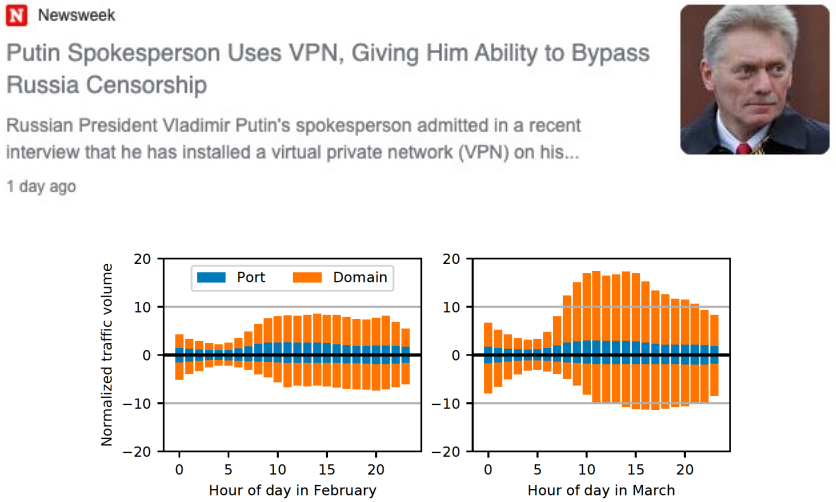


Figure 11: VPN traffic at the IXP-CE*

[1] See references in paper: [26, 34, 45, 61].
[2] See reference in paper: [22].

Research questions

1. How, when, and why do (or do not) corporate users* use VPNs?
2. How do they think VPNs work?
3. How do they see the impact of VPNs on the threat landscape?

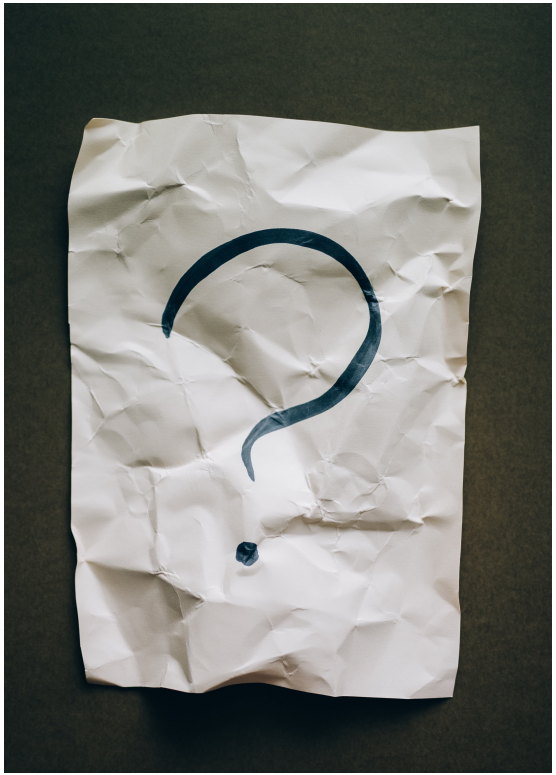


Photo by Olya Kobruseva

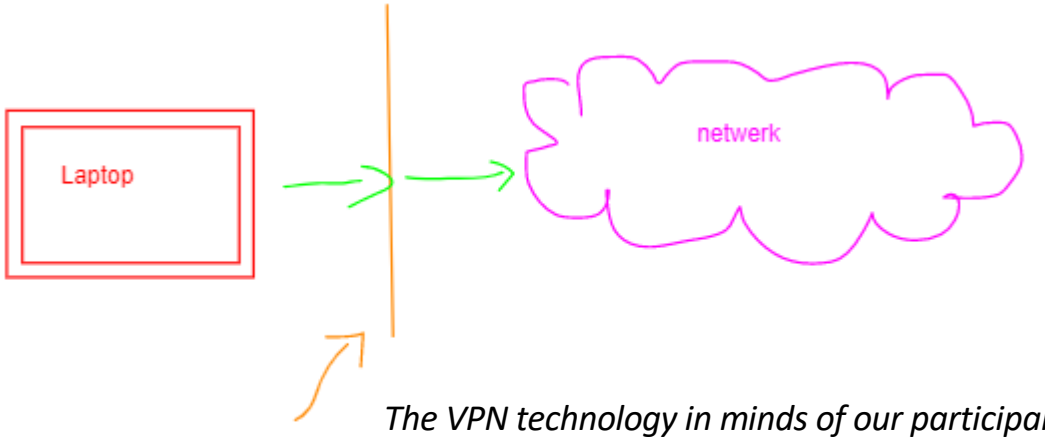
* corporate users = trained IT professionals + non-experts

(Research Method) How to get inside one's mind?

A mental model is a representation of a person's knowledge of a subject

- Elicitation techniques:
  - Semi-structured interview (reasoning + relationships between concepts);
  - Drawing task (to visualize interviewee's mental model);

- Three scenarios of a VPN usage:
  - From a home-office;
  - At a cafe/bar;
  - Sending email via the corporate VPN;



The VPN technology in minds of our participants. Illustration of the 'shield' metaphor by Expert 6.

Data Analysis

- Coding process -> Codebook
  - Open coding;
  - Axial coding;
  - Selective coding;
  - Model generation;
- Codebook reliability
  - 2 authors independently coded 3 interviews;
  - Krippendorff c-alpha-binary = 0.837 (after resolving disagreements);
- Final codebook
  - 86 codes
  - 4 core themes

Participants and the VPN they used

Who

- Employees of a Dutch office of a professional consulting firm;
- 7 non-experts
  - Legal, finance, and HR departments;
  - Employed in avg. 6 years in the firm;
- 11 experts in IT security
  - At least 2 years in IT department OR hold a relevant certification (e.g., CISSP, CISA, etc.);
  - Employed in avg. 4 years in the firm;

What VPN

- VPN supplied by a major network device vendor
- Custom white-labeled client
- Complete tunnel connection

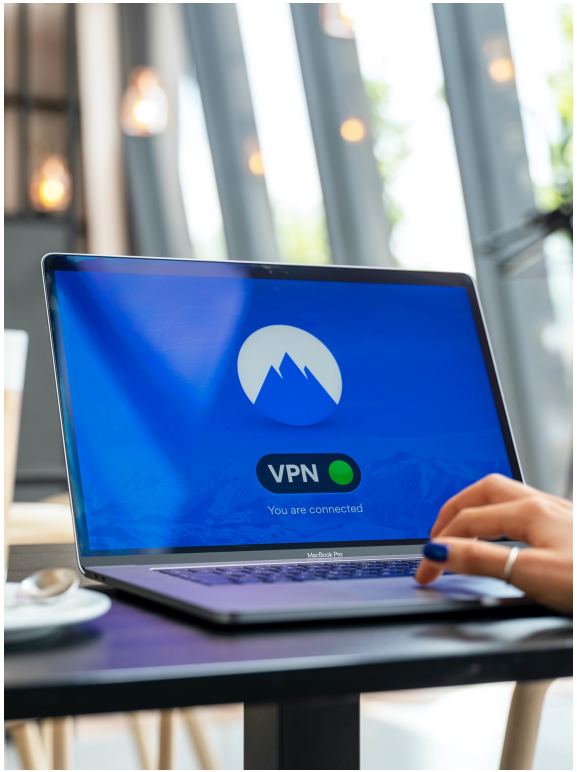
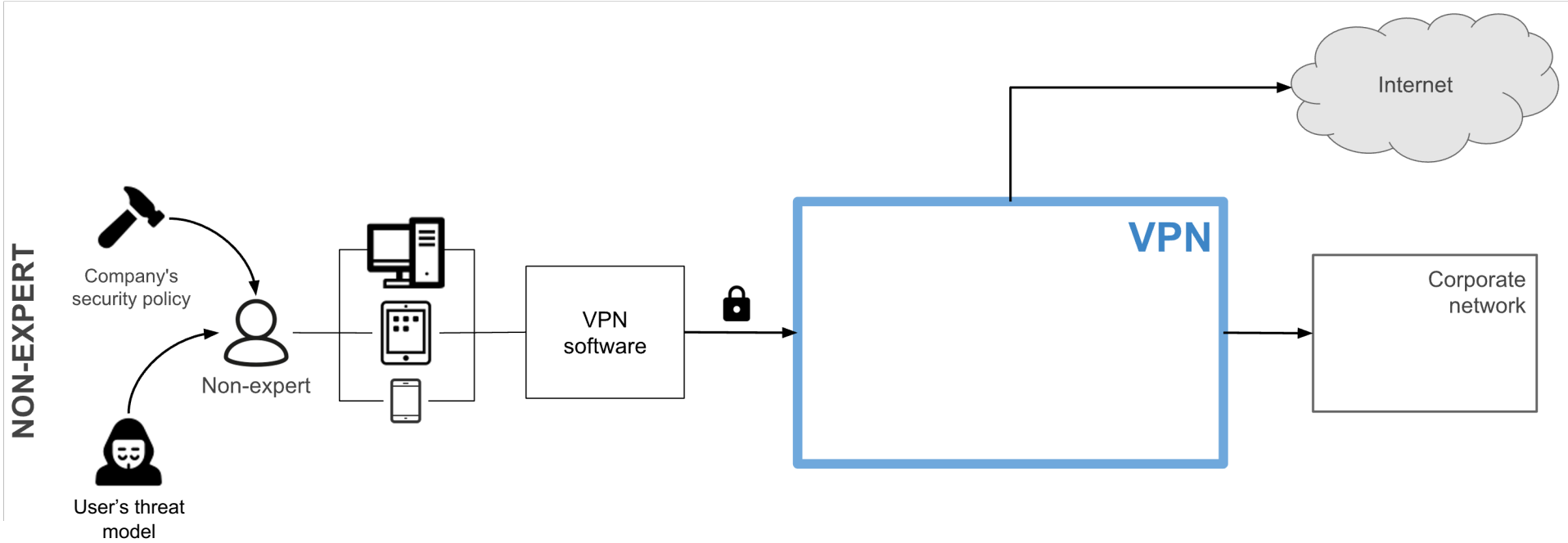


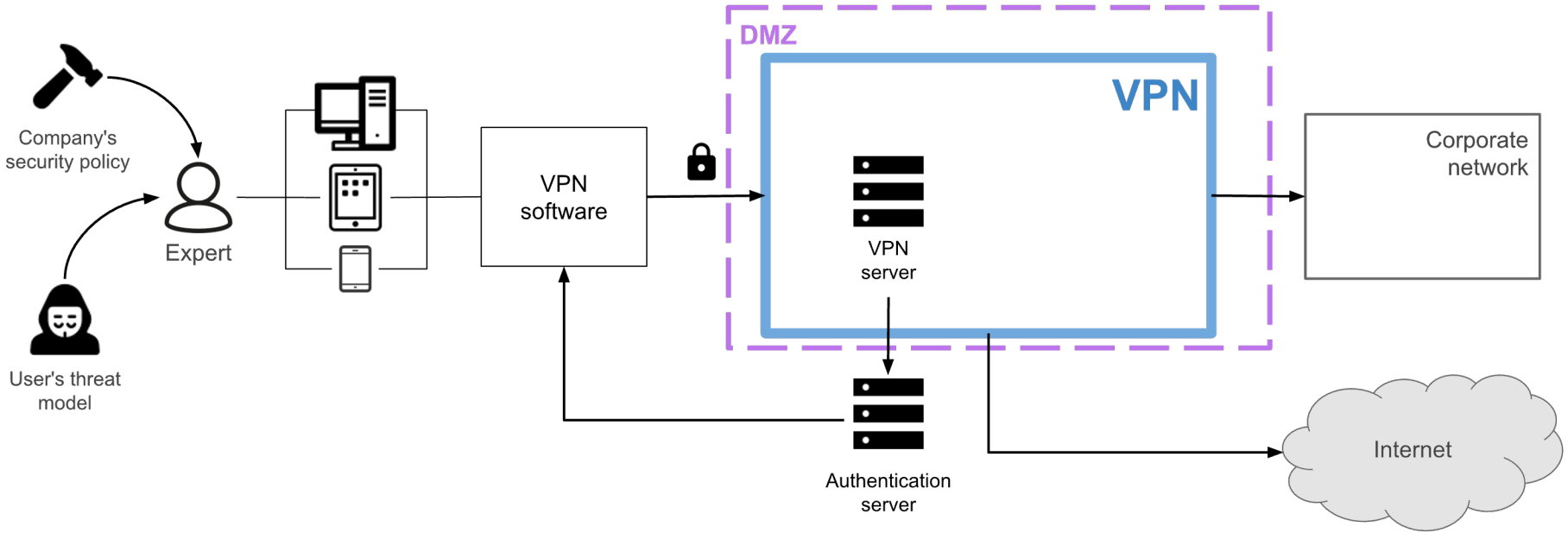
Photo by Petter Lagson

[Non-Expert Model] How a VPN works and used

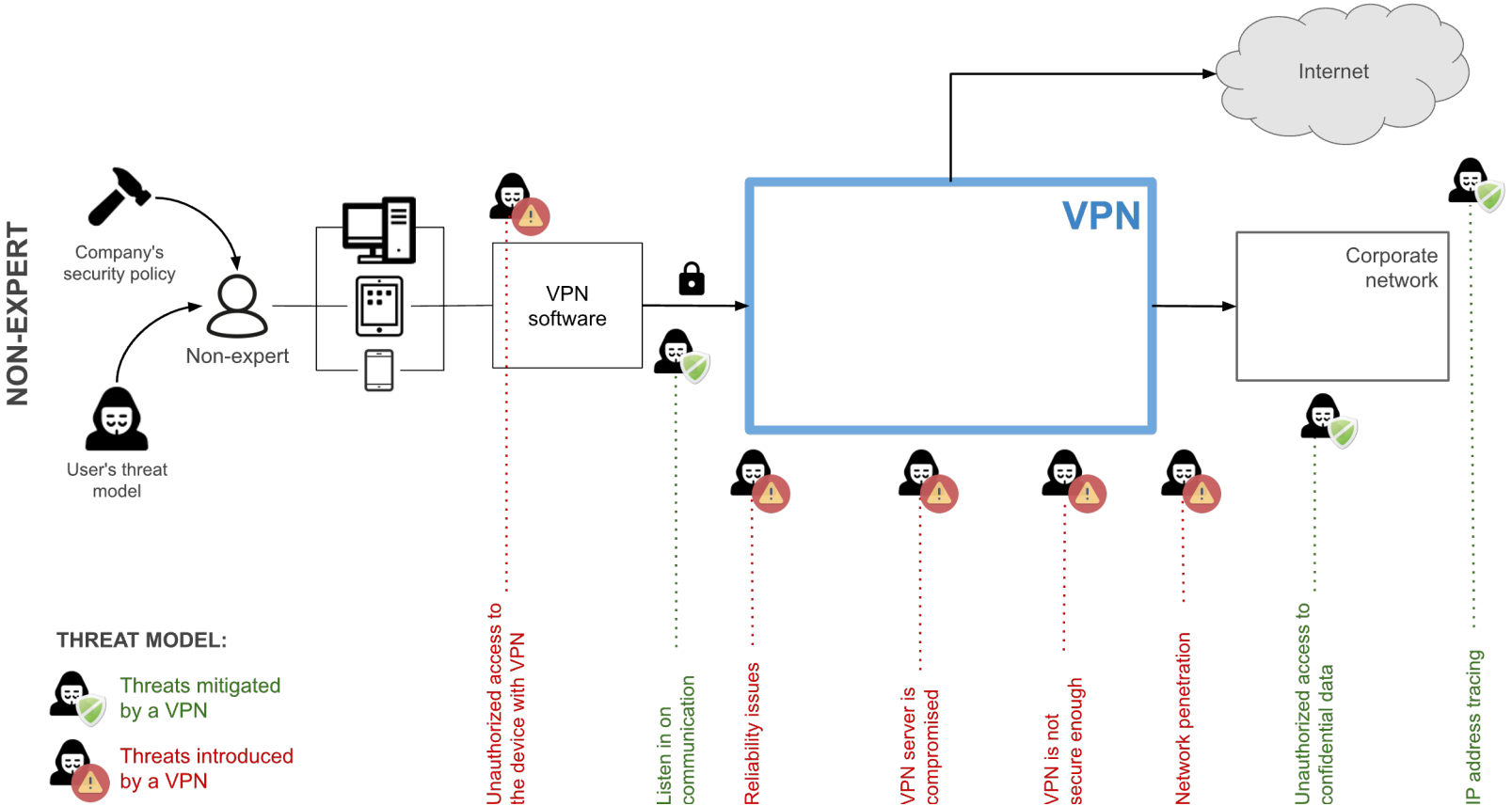


[Expert Model] How a VPN works and used

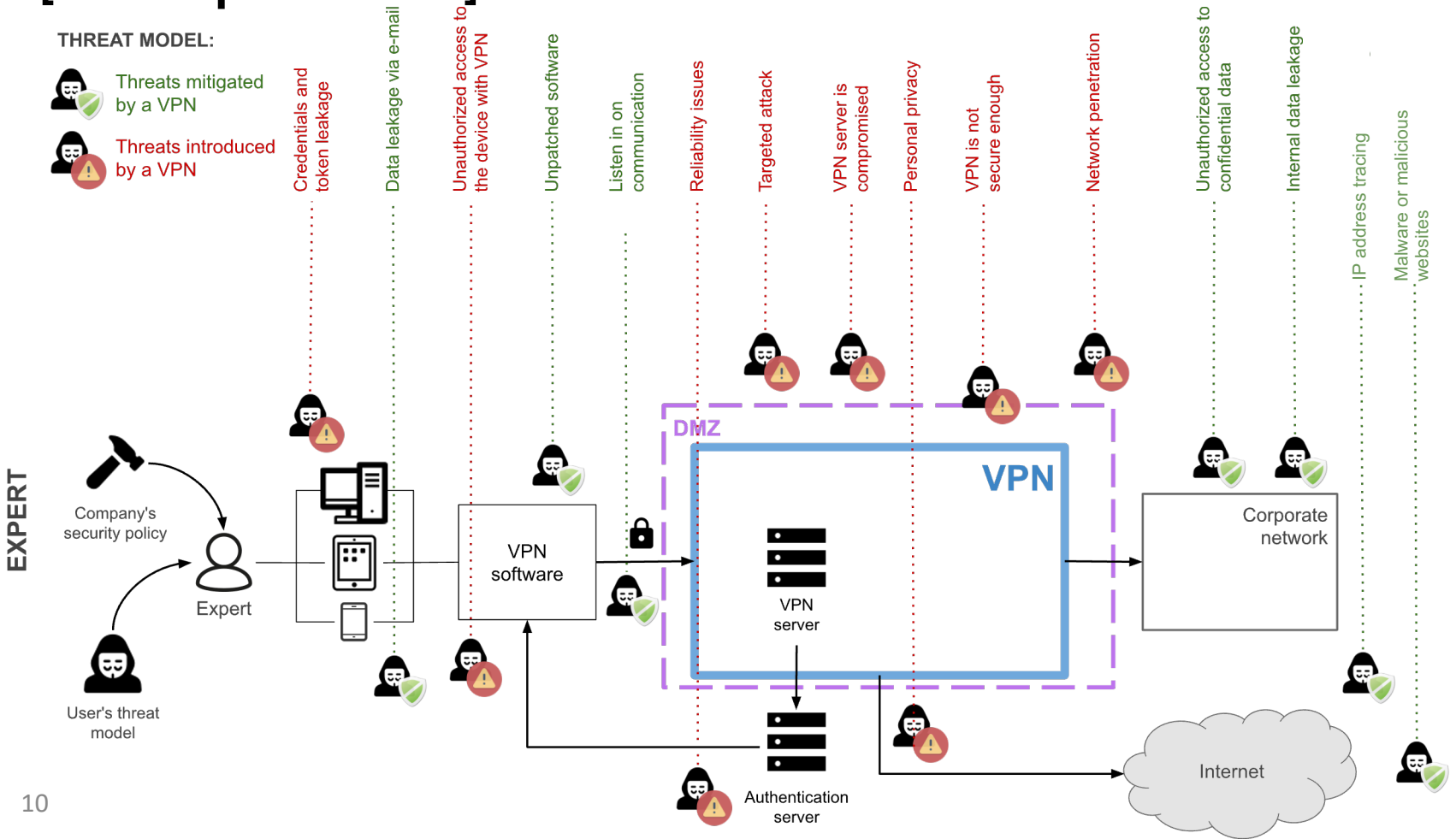
EXPERT



[Non-Expert Model] Threat model



[Expert Model] Threat model



Recommendations

- VPN Automation
  - make VPN usage invisible and the default for users
- Privacy Communication
  - accommodate a degree of private VPN use and communicate it to the employees proactively
- Device Management
  - Adjust device management solutions to securely work even without a VPN
- Technical Training
  - Focus on what people need to know based on mental models
  - Use the ‘tunnel’ metaphor to make training accessible

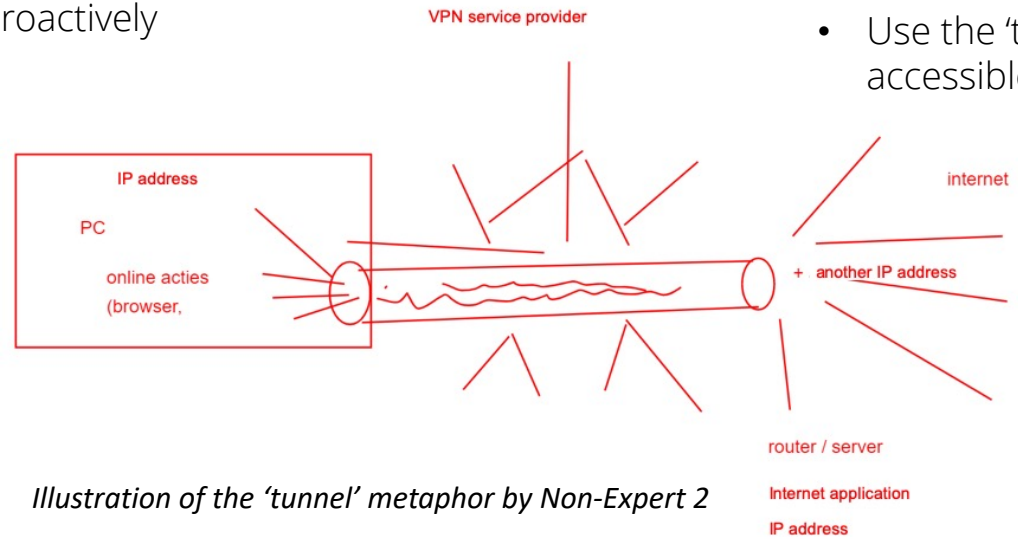


Illustration of the ‘tunnel’ metaphor by Non-Expert 2

Future Research

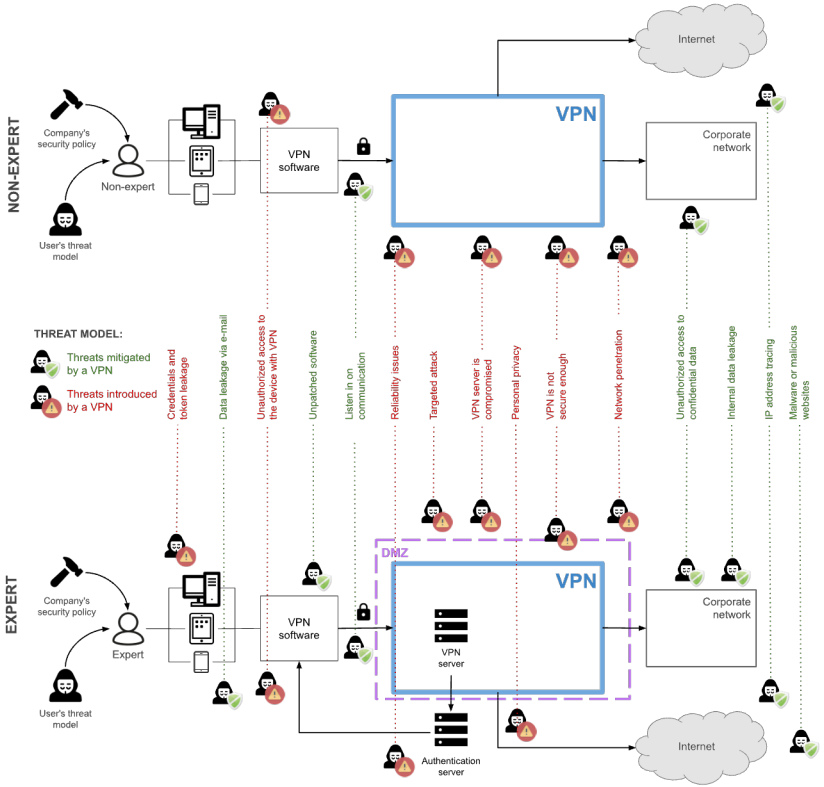
Photo by Startup Stock Photos

- Explore the privacy concerns made by experts in the context of privately used VPNs
- Trust interdependencies between end-users and their local Internet Service Providers (ISPs)
  - our VPN mental model of non-experts can serve as a basis for interview script
- Quantitative study of the use of VPNs in various contexts
- Empirical validation of the interventions based on our recommendations through controlled experiments

Summary

- At a high level, non-expert and experts have similar mental models of VPN technology;
- Experts have a deeper technical understanding of VPNs;
- Experts are also concerned about the privacy implications of using a corporate VPN;
- Experts found VPNs to be an integral part of fleet management and policy/compliance enforcement

- Automate VPN usage, improve privacy communication, and focus training on what people need to know following their mental models.



USENIX SECURITY 2022

Thank you for your attention!

Veroniek Binkhorst, Tobias Fiebig, Katharina Krombholz, Wolter Pieters, and

Katsiaryna (Kate) Labunets
[k.labunets@uu.nl]