EPFL

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

Computer Security (COM-301)
Interactive Exercises
Privacy

MCQ 2019

A VPN can hide the destination of your communication against an adversary looking at your local traffic. What would be the advantage of using Tor if a VPN can already do that?

A) To reduce latency
B) To eliminate traffic analysis attacks
C) To prevent trust centralization
D) To protect against weak cryptographic keys

Correct answer C
A) Anonymous communication systems like Tor generally increase latency
B) Tor is still susceptible to traffic analysis from global adversaries
D) Does not make any sense in this context

The grinch

The grinch wants to steal a bike, and wants to do so during Christmas eve. The grinch decides to go chimney-to-chimney during Christmas night and steal some of the presents delivered by Santa. The presents are “encrypted” with Santa’s special gift wrapping paper, and can only be opened on the morning of the 25th. The grinch does not have much space and can only bring home a limited amount of presents.

When looking at the “encrypted” presents, how can the Grinch maximize his chances to bring home a bike? Equivalently, how can he pick which gifts to steal and which ones to leave?

Propose a technique seen in class that Santa could use to prevent this.

The shape / weight is still observable. Similarly to a metadata analysis, the Grinch can eliminate small gifts, etc,...
Something related to padding could prevent such an attack by putting all gifts in a big box before wrapping them, so that they all have the same size.
Another technique could be to dismantle the big gifts (if possible) into smaller sized gifts.

Love Actually

Alabaster Snowball and Bushy Evergreen, two of Santa Claus' elves, are having a love affair, despite Santa's strict ban on relationships at work! To hide their relationship from Santa, Alabaster and Bushy live in separate houses in the Elf Village and exchange messages via the Tor network. The only problem is that because power supplies in the Elf Village at the North Pole are low and sending or receiving a message over Tor consumes a lot of power, every time the two exchange a message, the light in their respective houses flicker. Thus, the two elves try to exchange as few messages as possible.

One cold night, Alabaster sends a good night message to Bushy over Tor. The next morning Santa angrily storms into the elves' offices and shouts: "I knew it! Alabaster! Bushy! I said relationships at work are strictly forbidden! You thought that using Tor was enough to hide your conversations. You thought wrong."

Explain how Santa could have learned about the relationship of the two elves. Assume that Santa does not have any control over any of the Tor nodes through which Alabaster's and Bushy's messages were routed and that none of the other elves would ever give away their secret. Describe which weakness of the Tor network enabled Santa to learn this information.

Part 1: Santa conducted a traffic correlation attack. Santa can observe both endpoints of the conversation (analogue to a global adversary). Because the lights flicker when messages are sent and received, he can hence still infere who is communicating late at night.

Love Actually

The next day Pepper Minstix, the Head of Elf Security, approaches Bushy and Alabaster and offers them an alternative way to communicate. He has built his own anonymous communication system: Sekoittaa. Pepper has installed a server in each of the elves' houses. To relay a message anonymously, Sekoittaa uses onion encryption like in the Tor network. It first sends all messages to the server in Pepper's own house who delays forwarding of the message by ten seconds. From there, each message is sent over three randomly chosen other servers before finally being forwarded to its recipient. Unfortunately, however, the power supply problem still leads to the light in a house flickering when the house's server sends out or receives a message.

If Bushy and Alabaster had used Sekoittaa to exchange their messages, would their relationship have remained hidden from Santa? Justify your answer.

Part 2: No, Pepper's design likely would not defend against Santa's attack. Because messages are always delayed by a fixed amount and not properly "mixed" traffic correlation attacks are still possible.