CSE508 Network Security

5/4/2015 Anonymity

Michalis Polychronakis
Stony Brook University
Privacy

“The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.” [RFC2828]

Anonymity

“The state of being not identifiable within a set of subjects, the anonymity set.” [Pfitzmann and Köhntopp]

Very different from privacy:

An anonymous action may be public, but the actor’s identity remains unknown (e.g., vote in free elections)
SSL-busting code that threatened Lenovo users found in a dozen more apps

"What all these applications have in common is that they make people less secure."

by Dan Goodin - Feb 22, 2015 3:45pm EST

LATEST FEATURE STORY

Battlefield Hardline review: an odd, cops-and-robbers facade

New twists on old formula help in multiplayer, baffle in single player.
“Unauthorized code” in Juniper firewalls decrypts encrypted VPN traffic

Backdoor in NetScreen firewalls gives attackers admin access, VPN decrypt ability.

by Dan Goodin - Dec 17, 2015 6:50pm EST

An operating system used to manage firewalls sold by Juniper Networks contains unauthorized code that surreptitiously decrypts traffic sent through virtual private networks, officials from the company warned Thursday.

It's not clear how the code got there or how long it has been there. An advisory published by the company said that NetScreen firewalls using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are affected and require immediate patching. Release notes published by Juniper suggest the earliest vulnerable versions date back to at least 2012 and possibly earlier. There's no evidence right now that the backdoor was put in other Juniper OSes or devices.

"During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen devices and to decrypt VPN connections," Juniper Chief Information officer Bob Worrall wrote. "Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS."

A separate advisory from Juniper says there are two separate vulnerabilities, but stops short of describing either as "unauthorized code." The first flaw allows unauthorized remote administrative access to Juniper firewalls. The second allows attackers to send forged packets to Juniper firewalls, but requires a thumbprint when encrypted.
AUTHORITIES LAUNCH MAN-IN-THE-MIDDLE ATTACK ON GOOGLE
Submitted by percy on Thu, Sep 04, 2014

WHAT HAPPENED?

From August 28, 2014 reports appeared on Weibo and Google Plus that users in China trying to access google.com and google.com.hk via CERNET, the country’s education network, were receiving warning messages about invalid SSL certificates. The evidence, which we include later in this post, indicates that this was caused by a man-in-the-middle attack.

While the authorities have been blocking access to most things Google since June 4th, they have kept their hands off of CERNET, China’s nationwide education and research network. However, in the lead up to the new school year, the Chinese authorities launched a man-in-the-middle (MITM) attack against Google.

We begin the news about the MITM attacking GitHub in January 2013. To learn more from that attack, you’ll want to read here.

COMMENTS

Submitted by Marty on Mon, Sep 22, 2014
It’s amazing too pay a quick visit this site and reading the views of all colleagues on the topic of this post, while I am also eager of getting knowledge. Here is my page; effective weight, Marty.

Submitted by subway surfers ... on Sat, Sep 27, 2014
I’m gone to convey my little brother, that he should also pay a quick visit this web site on regular basis to obtain updated from most recent gossip.

Submitted by Merissa on Sun, Sep 28, 2014
I think the admin of this site is genuinely working hard in support of his website, because here every stuff is
French agency caught minting SSL certificates impersonating Google
Unauthorized credentials for Google sites were accepted by many browsers.

by Dan Goodin - Dec 9 2013, 2:05pm EST
Chinese attackers used the Great Firewall's offensive sister-system, named the Great Cannon, to launch a recent series of distributed denial of service attacks targeting the anti-censorship site, GreatFire.org, and the code repository, Github, which was hosting content from the former.

The first set of DDoS attacks hit GreatFire.org on March 16. On March 26, Github
Anonymous communication

Sender anonymity
The identity of the party who sent a message is hidden, while its receiver (and the message itself) might not be

Receiver anonymity
The identity of the receiver is hidden

Unlinkability of sender and receiver
Although the sender and receiver can each be identified as participating in some communication, they cannot be identified as communicating with each other
The internet was not designed for anonymity

Packets have source and destination IP addresses

Using pseudonyms to post anonymously is not enough…

Server always sees the IP address of the client

Need to hide the source IP address

Assuming no other PII is revealed (!) – OPSEC is hard
Stepping Stones: Anonymity

Proxies, relays, VPN servers

Server sees only the IP address of the proxy
Since the proxy cooperates, let’s also encrypt the connection to it

Sender anonymity against the server and network observers beyond the proxy

Also: receiver anonymity against local observers
All they can see is client ⇆ proxy connections
Encrypted tunnel hides the actual destination
Stepping Stones: Traffic Protection

Besides anonymity, the encrypted client ⇔ proxy channel offers protection against local adversaries.

The definition of “local” depends on the location of the proxy.

Users in the same LAN, employer’s admins, ISPs, governments, …

Protection against passive and active network adversaries (eavesdropping, MitM, MotS, …)

Policy and censorship circumvention

Parental controls, company-wide port/domain/content blocking, hotel WiFi restrictions, government censorship, …
What about other adversaries?

The proxy itself may be the adversary – can see it all!

Network observers beyond the proxy can see it all!

Adversaries who couldn’t eavesdrop before, now can: just set up a rogue proxy and lure users

End-to-end encryption is critical!
What about other adversaries?

A “global” adversary may be able to observe both ends

Traffic analysis: communication patterns can be observed even when end-to-end encryption is used
Eavesdropping vs. Traffic Analysis

Even when communication is encrypted, the mere fact that two parties communicate reveals a lot

Example: what can we learn from phone records?
   - Who communicated with whom and when
   - Activity patterns (periodic, time of day, occasional, …)
   - Single purpose numbers (hotlines, agencies, doctors, …)

*It’s not “just metadata”…*

Network traffic analysis can reveal a lot
Passive traffic analysis
Frequency and timing of packets, packet sizes, amount of transferred data, …

Active traffic analysis
Packet injection, fingerprint injection through manipulation of traffic characteristics, …

Examples:
Message timing correlation to learn who is talking to whom
Visited HTTPS web pages through structural analysis (number/size of embedded elements etc.)
SSH keystroke timing analysis

“Traffic analysis, not cryptanalysis, is the backbone of communications intelligence.”
— Susan Landau and Whitfield Diffie
Mix Networks [Chaum 1981]

Main idea: hide own traffic among others’ traffic

Originally conceived for anonymous email: Trusted remailer + public key cryptography

Additional measures are critical for thwarting traffic analysis: message padding, delayed dispatch, dummy traffic
Adding multiple mix relays allows for anonymity even if some relays are controlled by an adversary.

Deanonymization still possible if an attacker controls *all* relays of a circuit.
(aka. the Onion Router)

Low-latency anonymous communication network

Layered encryption: each relay decrypts a layer of encryption to reveal only the next relay

© Tor Project - https://www.torproject.org/about/overview.html.en
Worldwide volunteer network of 7K+ relays
  More than 2M daily users

Three-hop circuits by default
  Entry node, middleman, exit node
  Longer circuits can be built
  Multiple connections can be multiplexed
  over the same Tor circuit

Directory servers point to active Tor relays
  10 directory servers hard-coded into the Tor client
  Monitoring for mass subscriptions by potential adversaries
  (sybil attack)
Applications

User-friendly Tor Browser
  Additional measures to thwart web tracking and fingerprinting

TAILS (The Amnesic Incognito Live System) Linux distribution
  Forces all outgoing connections to go through Tor

Onion services: hide the IP address of servers
  .onion pseudo top-level domain host suffix
  Not always easy: misconfigurations and leaks may reveal the real IP address of the server

SecureDrop (originally designed by Aaron Swartz)
  Platform for secure anonymous communication between journalists and sources (whistleblowers)

Many more: OnionShare (file sharing), Ricochet (IM), …
**Hidden Services: 1**

**Step 1:** Bob picks some introduction points and builds circuits to them.

Alice

Bob

IP1

IP2

IP3

DB

Tor cloud
Tor circuit
Introduction points
Public key
One-time secret
Rendezvous point
Onion addresses are self-authenticating: derived from the service’s public key
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.
**Hidden Services: 4**

**Step 4:** Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.
Step 5: Bob connects to the Alice’s rendezvous point and provides her one-time secret.
Step 6: Bob and Alice proceed to use their Tor circuits like normal.
1 Million People use Facebook over Tor

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we’ve written previously it’s important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

This is why in the last two years we built the Facebook onion site and onion-mobile site, helped standardise the “.onion” domain name, and implemented Tor connectivity for our mobile app.
Censors want to block Tor

Directory servers are the easy target
   Block any access to them

Response: Tor bridges
   Tor relays that aren't listed in the main Tor directory
   Only a few at a time can be obtained on-demand (e.g., through email to bridges@bridges.torproject.org)
   Once known, adversaries may block them too…

Pluggable Transports
   Censors may drop all Tor traffic through deep packet inspection
   Hide Tor traffic in plain sight by masquerading it as some other innocent-looking protocol (HTTP, Skype, Starcraft, …)
FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

BY KEVIN POUlsen 09.13.13 | 4:17 PM | PERMALINK
For a year, gang operating rogue Tor node infected Windows executables

Attacks tied to gang that previously infected governments with highly advanced malware.

by Dan Goodin - Nov 14, 2014 10:30am EST

Enlarge / A flowchart of the infection process used by a malicious Tor exit node.
How Hackers Abused Tor To Rob Blockchain, Steal Bitcoin, Target Private Email And Get Away With It

Across October and November of last year, some unlucky users of the world’s most popular Bitcoin wallet, Blockchain.info, and one of the better-known exchanges, LocalBitcoins, had their usernames and passwords silently pilfered. They were robbed of significant sums, probably tens of thousands of dollars worth of the virtual currency, possibly more. Security-focused email services, Riseup and Safe-mail were also targeted by the same crew. And according to the man who witnessed the attacks go off last year, Digital Assurance director Greg Jones, it looks like buyers and sellers of dark markets were the targets.

The attackers used a tried-and-tested method to begin with, setting up a number of malicious exit relays on Tor. Legitimate exit relays act as the final jump from the anonymising Tor network, which loops users through a number of randomly-chosen servers across the world to protect their identity, onto the clear web. But any nefarious type who runs a malicious relay can use an encryption removal technique known as SSL stripping, where connections are
Detecting Traffic Snooping in Tor using Decoys

Expose unique decoy username+password through each exit node
Wait for unsolicited connections to the honeypot server using any of the exposed bait credentials
Detected Rogue Exit Nodes

30-month period: detected **18 cases** of traffic eavesdropping that involved **14 different Tor exit nodes**
Online Privacy and Anonymity: What Can We do?

Technical solutions exist
  Encryption
  Self-hosted services
  Anonymous communication
  …

But they are not enough
  Privacy vs. usability tradeoff
  Wrong assumptions
  Implementation flaws

*Many users are not even aware of privacy issues, let alone solutions*

*Protect the right of individuals to control what information related to them may be collected*
  *With technical means, not promises…*