Homework 4

Scott Ouellette

Scott_Ouellette@hms.harvard.edu

1.)

The US Computer Emergency Readiness Team (US-CERT) publishes what are called Technical Cyber Security Alerts and Vulnerability Notes and these documents alert users to potential threats to the security of their systems. Select a Technical Security Alert or Vulnerability Note published in the last twelve months that has a network related component to it and research the reported problem and the suggested solution (if one is available.) Analyze and describe the problem, and the solution paying close attention to the network related issues that it raises. We are interested in reading your analysis, and not a cut-and-paste of what is on the website. The listing of recent Technical Security Alerts can be found at: https://www.us-cert.gov/ncas/alerts and the listing of Vulnerability Notes is at https://www.kb.cert.org/vuls IMPORTANT NOTE: You should not select the Security Alerts related to the various DDOS attacks for analysis since they have been covered to such a large extent in the technical press.

I've chosen Vulnerability Note VU#144389 to report on. In short, VU#144389 describes a scenario with TLS where a given TLS implementation can allow for an unauthenticated remote party to obtain the TLS session key and be able to decrypt all of said implementation's TLS traffic. This vulnerability stems from the way an implementer could mishandle the padding within the RSA encryption standard PKCS #1's Client Key Exchange Message which is responsible for setting the premaster secret private RSA key. If implemented improperly, there are scenarios that can occur that would allow for an attacker to distinguish between valid and invalid messages further allowing for the use of these discrepancies to obtain the aforementioned pre-master secret key private RSA key. I've read that a common name for such an attack is knwon as a Bleichenbacher attack.

2.)

The following questions all relate to email. Answer each question in detail.

a). Explain the structure of the envelope, the header and the body of an SMTP message.

- The envelope in this case is the encapsulation mechanism that allows email traffic to be sent between MTAs (Mail transfer Agents). It is important to appreciate that the envelope isn't responsible for determining how the message is sent. The actual send done between MTAs can be done in many ways (HTTP, SMTP, a Vendor software). The header has lots of useful information. This information includes things such as: From, Subject, Date, To, Received etc. There are many headers used nowadays, but as a whole they describe the lifecycle of the piece of mail being transmitted. The body is simply the more human readable message that you want your receiver to interpret.

b). Explain how MIME is used to send non-ASCII, binary data (such as images) as an attachment.

- Originally, email was a text only deal. This fell short when folks wanted to start sending their .mp3s and other types of file formats. To be able to send a multitude of formats through email/SMTP MIME (Multipurpose internet mail extensions) and the notion of content types/content encoding was introduced. These are actually just more email headers that describe what is coming along in the envelope (Sounds pretty familiar to earlier learning about packets and protocol type fields etc.) and how said information has been encoded.

c). Give 2 examples of the differences between POP and IMAP.

- POP downloads email to your local machine and deletes it from the remote server. Think of going to physically pick up your mail from the **P**ost **O**ffice
- IMAP allows for the sync of email across many devices since it allows email to reside on remote servers.

d). What is SMTP relaying and why is it not a good idea? How can it be used maliciously?

- STMP relaying allows for email to be transmitted around the internet to other MTAs in a chain like fashion until a message is delivered. This is a bad idea because email/SMTP is inherently unreliable. There is no guarantee that said mail will be delivered between each "hop" (modern solutions do fancy things like retries and delivery receipts), but one can imagine that in a basic diagram the more MTA's "hands" that get on a message, the more room for failure of delivery.

3.)

Web browsers have a configuration field for a Proxy Server. Describe the technical operation of a proxy server and give at least two technical reasons why a company would implement a proxy server on their network.

- A Proxy server sits as an intermediary between two (or more) hosts forwarding (mainly) web traffic in between them. The functionality of a proxy server commonly known to the public is to "get around website blocks at work/school". What is really happening here is that the local institution's policies are being circumvented. Instead of a user making a request to a blocked `netflix.com`, they can send the request to a proxy server which, to the local institution is a perfectly valid, unblocked host, and said server will forward the request and the response back from `www.netflix.com` to the requesting host.
- A company could use a proxy server for a multitude of reasons. A few of them being:
    - As a initial layer of security. You could advertise the public IP of your proxy server and have it forward traffic to your webserver sitting behind some additional fortifications.
    - Load sharing. The single proxy could be responsible for forwarding traffic to the appropriate N hosts behind it
    - Caching files (I haven't looked into how this specifically works yet, but Len said it in lecture so it must be important)

4.)

a) Assume that you are using a PC at Harvard and that no machine or DNS at Harvard has ever communicated with a machine at Yale. Now, assume that your machine is trying to reach www.yale.edu. Describe the process used by your web browser, the computer it is running on, the local DNS server it is configured to use, and the multiple intervening DNS servers, in order to resolve the IP address for the machine at Yale.

First off, My computer must be configured to use DNS i.e. talk to some resolver (DNS Server). This can be done manually or automatically with DHCP. The configuration will end up pointing to at least one DNS root server (we'll see why below). When my client makes the request to www.yale.edu my resolver has no clue initially what to do so it needs to ask for some help. Since the DNS namespace is: hierarchical, a decentralized distributed "database", and our resolver has an idea of at least one server that knows about the "root namespace" our resolver can perform lookups in the following manner:

- Ask root server: "Who knows about `.edu`?" and gets a reply: `EDU DNS SERVER A`
- My resolver then asks `EDU DNS SERVER A`: "Who knows about the `yale` zone?" and gets a reply `YALE.EDU DNS SERVER X`
- My resolver then asks `YALE.EDU DNS SERVER X`: "What IP is the `www` host?" and gets an IP in reply `X.X.X.123`
- My resolver then discloses the IP of `www.yale.edu` to my computer then allowing it to do the usual HTTP GET to: `X.X.X.123`
- Its crucial to appreciate that my computer **ONLY** talks to the resolver its configured to use. Its that resolvers responsibility to do the DNS lookups

b) What is DNS caching? How and why is it used?

- DNS Caching would be done on any given resolver to avoid unnecessary lookups. Once a record has been looked up, it can be cached for quicker responses to the requesting client. There is a TTL associated with DNS records so that they can be purged appropriately.

5)

Determine the public IP address of your Internet connection at your home, school, or office, and then identify the Autonomous System Number (ASN) that corresponds to your public network address. You can use the various tools we have demonstrated in lecture to learn your public IP address and the corresponding ASN.

a) What is your public IP address and what is the AS number for this network?

- `134.174.140.174`
- `AS40127`:
  - Country: US
  - Registration Date: 2006-07-27
  - Registrar: arin
  - Owner: LMANET - Longwood Medical and Academic Area (LMA), US

b) In order to communicate with the rest of the Internet, the autonomous system of which you are a part, connects to other autonomous systems. For example, Harvard's AS number is AS1742 and two of its upstream connections are to AS numbers ASN174 (Cogent Communications) and AS3356 (Level-3 Communications.) Identify two upstream autonomous systems that are connected to the autonomous system you are part of (as identified in part a.) What are the names and ASN of these two upstream autonomous systems?

- `AS11164`:
  - Country: US
  - Registration Date: 2014-07-11
  - Registrar: arin
  - Owner: INTERNET2-TRANSITRAIL-CPS - Internet2, US
- `AS1742`:
  - Country: US
  - Registration Date: 1992-02-19
  - Registrar: arin
  - Owner: HARVARD-UNIV - Harvard University, US

6.)

In February 2015 security researchers discovered that Lenovo had pre-installed adware software on some specific models of their computers that made the machines very vulnerable to TLS/SSL spoofing attacks without a warning to the user. (As you know TLS/SSL is used to encrypt traffic in HTTPS.) This meant that these systems were vulnerable to a man-in-the-middle (MITM) attack which would allow an attacker to redirect a web request without warning, and to intercept and read supposedly secure HTTPS traffic between the browser (such as Chrome or IE) and a server. The US-CERT security alert about this is at: https://www.us-cert.gov/ncas/alerts/TA15-051A Given the large amount of press coverage about the problem at the time, it is not a surprise that some of the details and information that was published was confusing and contradictory. Review the literature and technical reports on the problem and write up a succinct description of the problem including a technical explanation of how an attacker would take advantage of the adware software that had been installed. Your description should be in your own words (i.e., not a cut-and-paste of other material) and should be one page or less (exclusive of any diagrams.)

As a starting point you might want to review the following articles:

- http://tinyurl.com/cscie40b
  - https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops
- http://tinyurl.com/cscie40c
  - https://blog.mozilla.org/security/2015/02/27/getting-superfish-out-of-firefox/
- http://tinyurl.com/cscie40d
  - http://www.networkworld.com/article/2887293/superfish-security-flaw-also-exists-in-other-apps-nonlenovo-systems.html
- http://tinyurl.com/cscie40e
  - https://www.facebook.com/notes/protect-the-graph/windows-ssl-interception-gone-wild/1570074729899339

The underlying problem with the Lenovo laptops in this case was that adware software called Superfish came pre-installed on some laptops, and this software installed a trusted root CA certificate for itself. It did this so that some spying could be done on user's web requests to provide targeted advertising. By doing this they essentially were doing a man-in-the-middle attack against their users. All

web traffic from the user would be caught by the Superfish software, decrypted, read/utilized, re-encrpyted and then passed along to the browser. The scary part here is that according to the webbrowser this was a completely legitimate operation due to the afformentiond trusted root CA certificate that the Superfish software installed. The common user would have no clue this was going on (unless they we're savvy enough to interpret where some of their targeted advertisments were coming from)

Superfish used a software library called: Komodia Redirector to do the HTTPS traffic decryption among some other things. Come to find out, this software was vulnerable to attacks! Specifically the Komodia software's root CA certificates that it installed used easily obtainable hard-coded private keys! An attacker could take advantage this vulnerability in the underlying Komodia software to spoof HTTPS websites and intercept HTTPS traffic on affected systems.