

Side-Channel Attacks

Ganesh Ananthanarayanan

7th April 2008

1. Definition

Today's lecture was on side-channel attacks in security systems. Loosely, a side channel attack can be defined as *information gained from details of a system's specific construction, not its conceptual algorithms*. Examples of side-channel information that can be used to launch attacks include timing difference, power consumption and optical signals. A related definition in this context is that of covert channels. It can be defined as *unanticipated means of communication*. This includes any sort of communication that the security system was not expecting. Note that an encrypted channel between an attacker and a compromised node does not count as a covert channel.

2. Information Flow in the Peer-Reviewing Process

This paper was published in 2007 and shows how a reviewer's anonymity in the peer-reviewing process can be compromised by malicious postscript documents.

- A paper submission in postscript (ps) is essentially like submitting a program. Implementation of ps allows information, possibly private, to be passed back to the person who submitted it using environment variables.
- Covert channel is used to communicate the information back to the guy who submitted the paper.
- Bizarre: Pdf files contains Javascript code in them!

3. Remote Timing Attacks are Practical

This paper was published in 2003. As the title goes, this paper proves that remote timing attacks are practically feasible.

- Typically, for performance reasons, multiplication and modulo arithmetic algorithms have speed hacks. While this generally results in significant performance improvements, this leaves them open to carefully crafted attacks on these optimizations.
- Figure 1 in the paper is the basis of the attack discussed in this paper. This graph talks about the time taken for the Montgomery reduction for various inputs. For values of the input closer to p or q , the factors used in RSA. If an attacker knows p or q , the game's over!
- The high-level idea in the attack is to do a few trials until you find points on either side of the drop in the graph. The value of q is extracted bit by bit. Say g is the input given to the system and let it be ABCDE000000 at any point in time. The bits marked in alphabets have already been figured out. The next input would be g_{hi} : ABCDE100000. Check if g and g_{hi} are on the same side or opposite sides of the curve (Figure 1). If you cross it, the bit is 0.
- It is neat that the paper demonstrates its ideas conclusively.
- Network characteristics:
 - Network should not to have a lot of jitter/variance and should exhibit fairly uniform characteristics. This is conceivable in the scenario of LANs especially if the attack is launched at unearthly hours.

- Is this realistic for WANs? It is not hard to imagine a helpful TCP variant that has its timestamps in microseconds. If we use this TCP variant, the server automatically measures the time for the attacker!
- The moral of the story is that often optimizations introduced in cryptographic algorithms for performance reasons lead to side channel attacks.

4. Information Leakage from Optical Emanations

This paper was published in 2002 and extracts information from optical signals.

- There is a degradation of the optical signal as the distance from the source increases. Figure 4 in the paper plots this clearly.
- Modems generally have LEDs as indicators of their various states. The optical signals from these LEDs can be used to gather information about the modem and its state – if it is on or off, what is the load on it and even the traffic characteristics.
- The other experiment is to extract the information on a monitor. The experimental set up has a Cathode Ray Tube (CRT) with a white board. A photo multiplier looks for flickers as the CRT sweeps the screen. This information can be used to reconstruct the text.
- Next month's IEEE S&P conference has attacks that read the display off people's eyeballs, teapots and spoons!

5. Other Examples

Now we discuss other examples of side-channel attacks.

- **Scanning by IP spoofing**
This is a side-channel attack that has been employed in real attacks. The IP identifier (IPID) in a host is incremented for an incoming SYN-ACK but not for a RST. This can be used to check if there are listeners on a port on a victim. An attacker has a steady packet exchange with a patsy and sends a connection request (SYN) to the victim with the patsy's address as the source. The victim either responds with a SYN-ACK or an RST depending on whether a service is running or not and the attacker can note the difference in the IPIDs and infer accordingly.

For a detailed description refer to <http://www.icir.org/vern/papers/norm-usenix-sec-01.pdf>, Section 5.1.

- **p0f**
This attack looks at traffic (live or traces) particularly SYN, SYN-ACK, RST and extracts the following information – window size, initial TTL, SACK, window scaling, order of options etc. This data can be used to extract 163 different types of systems!
- **Cuisine poll**
A website had voting options where people could vote between Italian or British cuisines. The poll was initialized with 500,000 votes for each of the categories. The challenge for the Internet security community was to design a system that resulted in 90% of the votes in favor of British cuisine by the end of the month.
 - The voting was done via an interesting UI that made automation of the process a difficult task. There were two boxes with images in them and users had to drag their

choice (British or Italian) in to the box where the box was specified by the image in it. For example, if there were two boxes with images of dog and paper in it, the instruction would tell the user to “drag your option into the box with the dog”.

- Note that the count for a cuisine goes down on a wrong vote.
- Brute-force Attack: The image of “British cuisine” and “Italian cuisine” can be learnt because they are static.
 - Drag the British cuisine option every time to the box on the left.
 - The number of image categories was finite.
 - The count of both the cuisines was displayed after every vote – use this as the feedback to learn the image categories.
- Feedback is the culprit for side-channel attacks to learn the parameters of the system – moral reinforced!
- More details can be found here: <http://www.icir.org/vern/tmp/SideChannels.ppt>.

6. General Comments

- Feedback/debugging information is the culprit. This acts as crucial directives for an attacker to refine his inputs. The debugging information is often an indication of whether he is on the right path or not.
- Specification vs. Implementation: Even though a specification for a certain system might be strong and secure, its effectiveness is completely at the hands of the implementation. Different implementations have different bugs, some of which can be critical.
- Physical Proximity: Certain classes of side-channel attacks assume physical proximity, e.g., the optical signal attacks for modems. It is arguable if they are feasible in practice and a follow-up study regarding the feasibility of such attacks would be useful.