CMPSCI 630 Systems **Spring 2017**

Lecture 10

Lecturer: Emery Berger *Scribe: Karthik Anantharamu*

10.1 Covert channels & Security

Covert channels are the hidden channels through which confidential information may be leaked. Regular channels transfer information through a legitimate mode of information transfer, like a read/write or network I/O. Covert channels usually leak some information so that an attacker may infer something about data which he cannot directly access using a regular channel. For example, temperature and radio frequency of a device are covert channels.

10.1.1 Timing attack

Timing attack is a covert channel attack that allows one to compromise a system by analyzing the time it takes to execute cryptographic algorithms. Because algorithms behave differently for different inputs, it is possible to identify the sequence of steps taken by an algorithm only by providing different inputs and measuring the time it takes to get back a result. For example, it is possible to guess password based on character inter-arrival times. Software run on CPU with data cache exhibit timing variations which can also lead to resource leaks.

10.1.2 Row-hammer attack

By repeatedly writing to a specific location in memory in a certain pattern, it is possible to alter the contents of neraby memory locations. This attack is called as row-hammer attack. Rapid row activations may alter the state of a victim row in memory, leading to memory corruption, information loss or many other side effects.

10.1.3 Buffer overflow & Stack smashing

Buffer overflow happens when a program overruns a buffer and writes to an adjacent memory location. For example, if buffer overflow writes a file path to a string buffer and the neighboring memory contains the location of a file to be removed, the program may remove a different file altogether.
In stack smashing, it is possible to overwrite a buffer until the stack return address is overwritten. The new return address may point to malicious code. Similarly, on a heap, it is possible to read the content of neighboring objects and compromise information.

10.1.4 Morris worm

This was one of the first worms distributed through the internet. It used a series of exploits to compromise a system and propagate further. It was designed to be self propagating. A critical bug in the worm was that,

as it self-replicated, it did not check whether the other system is already running a copy. The program was too quick in propagating itself and blocked the internet due to its self-propagating nature.

10.1.5 Shellcode & vtable injection

In shellcode injection, buffer overflow is crafted in such a way that a command shell is started and the attacker can then execute commands. A related attack is vtable injection, where function pointers in vtable are modified to point to malicious code using shellcode injection. When a particular method is to be executed, malicious code is executed instead.

10.1.6 Trojan Horse & Viruses

Trojan horse is a malicious program disguised as a benign program. Viruses are malware that install by shemselves. They may then do something malicious, or may even compromise user data. A **drive-by attack** is unintentional download of a virus into our system. Typically, a vulnerability is used to trigger this download.

10.1.7 Heap spray & NOP slide

Heap spraying is a kind of attack to execute arbitrary code by placing a specific sequence of bytes at a predetermined location in memory. Commonly, this is achieved by creating large number of objects, filling them with NOP. This leads to a NOP slide - a situation where a sequence NOPs are ignored and the CPU instruction flow simply slides across NOP until malicious code is encountered.

10.1.8 Information & Control flow

Information flows from various forms to various other forms. Information downloaded from the internet may be saved to a file on disk. Information read from a file may be sent over the network. Information propagates from source to sink. Quantative information flow measures how much information flows. Perl has a taint mode flag that tracks information flow from dangerous sources, like information read from the internet. In taint mode, any attempt to save information read from the internet will fail as it is considered dangerous. A sanitizer may be used in such cases to ensure that incoming data is not malicious. Control flow is the flow of a program control. Sometimes, this can lead to implicit information flow. It is possible to break taint using control flow while still carrying some information about tainted data. Because taint spreads exponentially, rapid spread of taint is termed taint explosion. Just like sanitizer, a declassifier checks outgoing data to ensure that nothing confidential is being leaked. "Doppelganger" approach runs two copies of a program, one that works with genuine data and the other that replaces certain calls (like disk read) to return random data. If the output produced by both the copies match, no information from source is being leaked. If not, some information from source is being leaked. Further transmission of data can be then blocked.

10.1.9 SSL

SSL uses asymmetric encryption like RSA so that a man in the middle attack and eavesdropping is not possible. However, it is still possible for a service provider to infer which websites and how many times one is visiting.

10.2 Anonymity - Tor

Providing anonymity and latency guarantee together is difficult as it depends on the number of servers and hop count. Tor is an implementaition of onion routing. Messages are encapsulated in layers of encrypion just like layers of an onion. The initiator contacts an entry node for connection. Using this, the initiator can send an encrypted message to a second node that the first node cannot decrypt. Here, the second node doesn't know if the entry node or any other node is an initiator and anonymity is preserved. However, it is possible to do correlation attacks in Tor. If there are a million computers but only two of them have active network I/O one after the other, it is easy to correlate that these two machines are communicating with each other. Their communication is not anonymous anymore. A large crowd is required for ensuring anonymity.