Security I: Supervision 3

Daniel Chatfield (dc584)

May 20, 2015

20. Read Ken Thompson: *Reflections on Trusting Trust*, Communications of the ACM, Vol 27, No 8, August 1984, pp 761-763 and explain how even a careful inspection of all source code within the TCB might miss carefully planted backdoors.

> Inspecting the source only helps you if you then compile from the source, otherwise there is no guarantee that the binary on your machine is made from the same source you are inspecting.
>
> Compilation requires a compiler, since a rogue compiler can simply add a trojan to any program it compiles it is necessary to trust the compiler. Inspecting the source of the compiler is clearly not sufficient as the source will be compiled with the compiler itself.

21. You are a technician working for the intelligence agency of Amoria. Your employer is extremely curious about what goes on in a particular ministry of Bumaria. This ministry has ordered networked computers from an Amorian supplier and you will be given access to the shipment before it reaches the customer. What modifications could you perform on the hardware to help with later break-in attempts, knowing that the Bumarian government only uses software from sources over which you have no control?

> Depending on how much comparative value is placed on remaining covert and gaining intelligence I would perform some of the following:
>
> - Install a GSM keylogger in the keyboard
> - Install custom firmware on the network chip such that whenever packets are sent to an IP address that belongs to Amoria the unused IP fields are used to carry some data from disk or ram for interception.
> - Install custom firmware on the hard drive such that when a sufficiently random string is encountered it will, for the next x seconds give some predetermined value for the password file.

22. The Bumarian government is forced to buy Amorian computers as its national hardware industry is far from competitive. However, there are strong suspicions that the Amorian intelligence agencies regularly modify hardware shipments to help in their espionage efforts. Bumaria has no lack of software skills and the government uses its own operating system. Suggest to the Bumarians some operating system techniques that can reduce the information security risks of potential malicious hardware modifications.

> I'm not sure what an operating system can possible do to protect against completely compromised hardware. It can't put anything secret in RAM since that can be compromised and yet at some point the data would have to be decrypted so that it could be used.
>
> I did think you could have a permutation function over the memory addresses to randomize it, but such a function would itself have to be stored in RAM.

32. The log file of your HTTP server shows odd requests such as

```
GET /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+C:\
GET /scripts/..%u002f..%u002fwinnt/system32/cmd.exe?/c+dir+C:\
GET /scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+C:\
```

Explain the attacker's exact flaw hypothesis and what these penetration attempts try to exploit.

(Is there a connection with the floor tile pattern outside the lecture theatre?)

> The attacker is checking to see whether the web server allows traversing up a directory and whether it parses non-standard unicode escape sequences as forward slashes.
>
> If it does and the webserver simply executes the script referenced by the URL then this will execute a command prompt with a command to list the directory contents of the root directory of the C drive.

2004 Paper 3 Question 9

33. Introduction to Security

(a) Explain briefly mechanisms that software on a desktop computer can use to securely generate secret keys for use in cryptographic protocols. [5]

It can take multiple sources of random data like time between interrupts, key presses, mouse movement etc. to create an entropy pool from which a pseudo random bit stream generator is seeded.

(b) Give *two* different ways of implementing residual information protection in an operating system and explain the threat addressed by each. [5]

Doesn't appear to be on the course anymore

Secure delete files When a file is deleted then overwrite it several times to ensure that the data could not be accessed by a third party later with access to the drive.

Zero registers on switch When the operating system performs a context switch it should zero the registers to prevent data leaking from one process to another.

(c) Consider the standard POSIX file-system access control mechanism:

i. Under which conditions can files and subdirectories be removed from a parent directory? [2]

If write access for the parent directory is present. If Write access for the file being deleted is present.

ii. Many Unix variants implement an extension known as the "sticky bit". What is its function? [2]

When the sticky bit is set, only the file/directory owner or root can rename or delete the file.

iii. On a POSIX system that lacks support for the "sticky bit", how could you achieve an equivalent effect? [2]

Not sure.

(d) VerySafe Ltd offer two vaults with electronic locks. They open only after the correct decimal code has been entered. The VS100 – a low-cost civilian model – expects a 6-digit code. After all six digits have been entered, it will either open or will signal that the code was wrong and ask for another try. The VS110 – a far more expensive government version – expects a 40-digit code. Users of a beta-test version of the VS110 [4]

complained about the difficulty of entering such a long code correctly. The manufacturer therefore made a last-minute modification. After every five digits, the VS110 now either confirms that the code has been entered correctly so far, or it asks for the previous five digits again. Compare the security of the VS100 and VS110.

> The VS100 requires a six digit code and thus there are 10^6 different permutations.
>
> The VS110 expects 8 5-digit passcodes and thus a user only has to try 10^5 combinations for each block and thus a total of 8×10^5. Therefore the VS100 provides more security.

34. Do software updates increase or decrease risk of successful attack?

> Software updates provide a useful mechanism to keep software up to date with latest patches which prevent security vulnerabilities from being exploited. The update procedure is itself prone to attack and a vulnerability in it could be quite disastrous but the benefits far outweigh the risks.

Introduction to Modern Cryptography Chapter 3

21. Let $\prod_1 = (Gen_1, Enc_1, Dec_1)$ and $\prod_2 = (Gen_2, Enc_2, Dec_2)$ be two encryption schemes for which it is known that at least one is CPA-secure. The problem is that you don't know which one is CPA-secure and which one may not be. Show how to construct an encryption scheme $\prod$ that is guaranteed to be CPA-secure as long as at least one of $\prod_1$ or$\cdot$ $\prod_2$ is CPA-secure. Try to provide a full proof of your answer.

> Not sure whether this is sound.
>
> Let X be a random sequence of bits that is the same length as the message. Let $Y = m \oplus X$. Neither X or Y reveal anything about the plaintext individually. These can then be put through the 2 schemes individually.