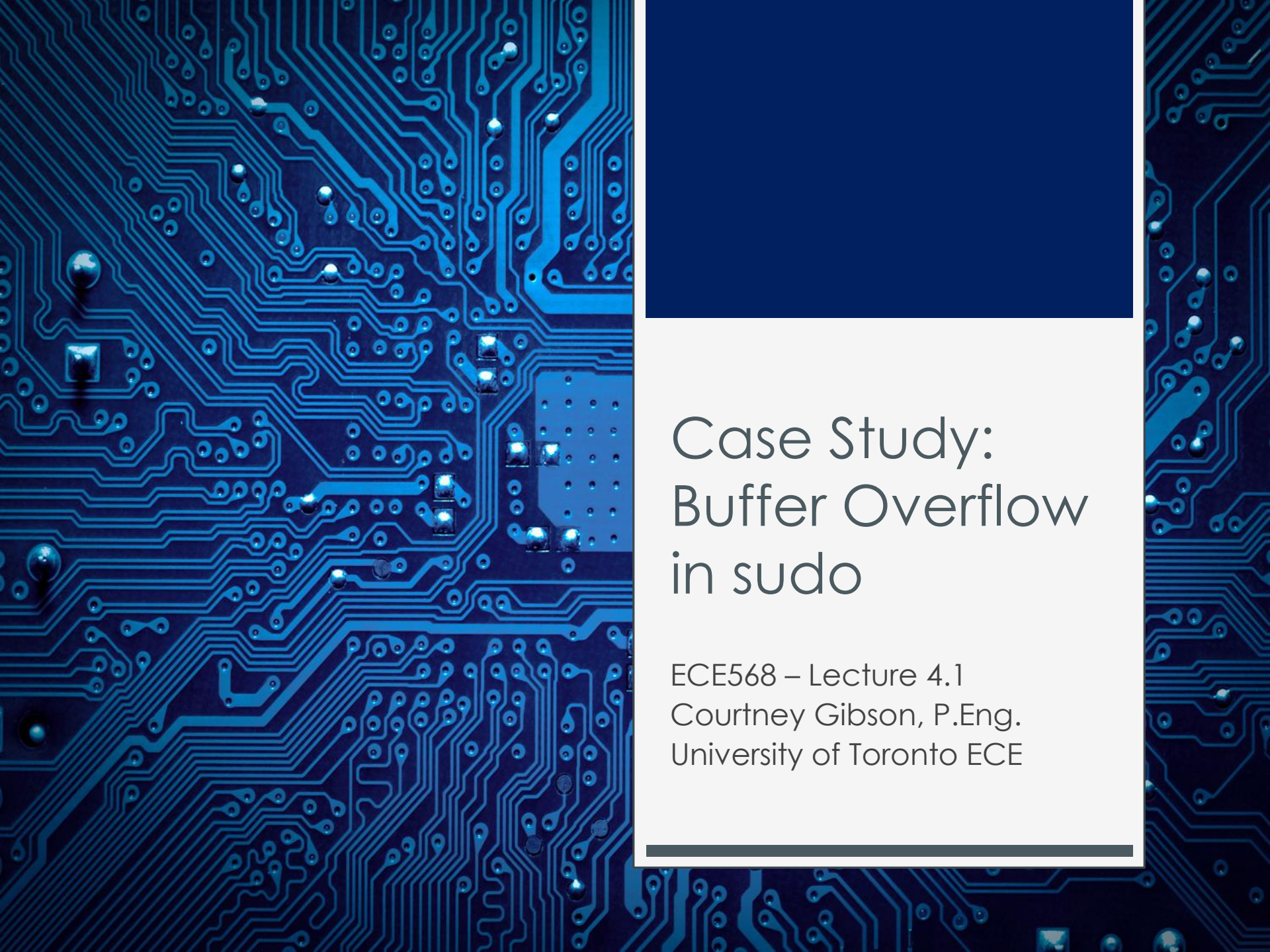


Case Study: Buffer Overflow in sudo

ECE568 – Lecture 4.1

Courtney Gibson, P.Eng.
University of Toronto ECE

sudo

- Used to allow **non-root users** (with appropriate permission) to execute commands as if they were root.
- An example of a **setuid** program. (Other examples are passwd, etc.)

$ **sudo** reboot --poweroff now

CVE-2021-3156

- Made public January 26, 2021
- Heap-based buffer overflow in **sudo**
- Exploitable by any local user, without authentication
- Will give root access
- Vulnerability was introduced in **July 2011** (versions 1.8.2 to 1.8.31p2 and 1.9.0 to 1.9.5p1)
- Exploits demonstrated on Ubuntu, Debian and Fedora
- Second bug discovered on January 23, 2021 that makes the vulnerability easier to exploit

CVE-2021-3156

- **sudo** starts by modifying the command-line arguments (in argv) by concatenating all command-line arguments and escaping all meta-characters with backslashes.
- Later, for logging purposes, it builds an array on the heap called *user_args* and copies in the contents of *argv*, while unescaping the meta-characters.
- Unfortunately, there's a bug… if any command-line argument ends in a single backslash ('\') then the argument's null terminator (0x00) gets "unescaped" and the code that is building *user_args* keeps copying out-of-bounds characters onto the stack.

CVE-2021-3156

```
$ sudoedit –s '\' `perl –e 'print "A" x 65536'`
malloc(): corrupted top size
Aborted (core dumped)
$
```

- ✓ They attacker controls the size of the *user_args* buffer that they overflow
- ✓ They can independently control the size and contents of the overflow itself: the last command-line argument is followed by the environment variables

CVE-2021-3156

An attacker has at least five exploit options:

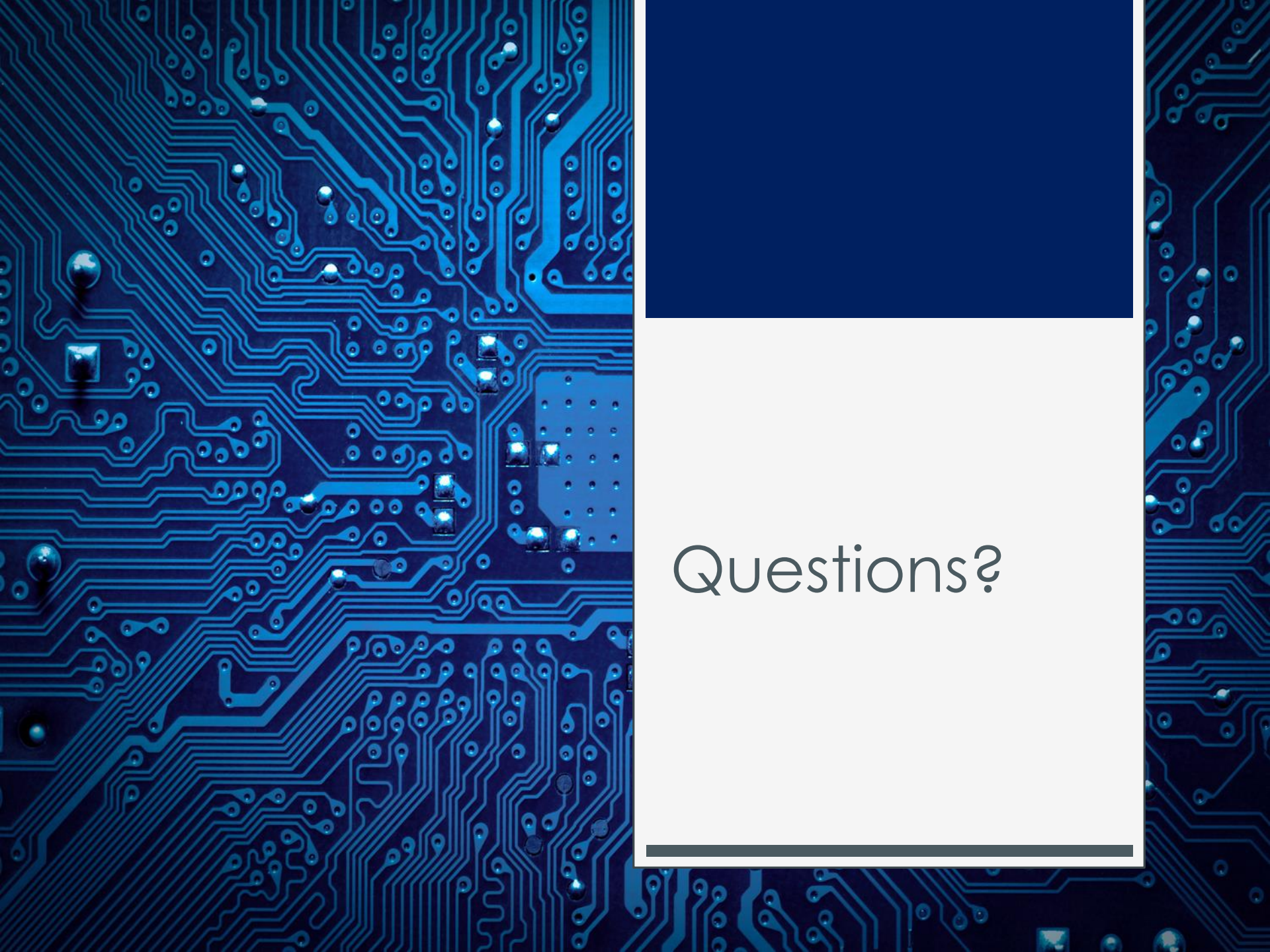
- ✓ Overwrite the next chunk's memory tag (same as use-after-free)
- ✓ Function pointer overwrite within one of **sudo**'s functions (*process_hooks_getenv()*)
- ✓ Dynamically-linked library overwrite (modify a memory structure, to change a reference to "libnss_systemd.so.2" to something else)
- ✓ Race condition, related to a temporary file that sudo creates
- ✓ Overwrite the string "/usr/sbin/sendmail" on the heap with the name of another executable

Further Reading

For more information:

CVE-2021-3156: Heap-Based Buffer Overflow in Sudo (Baron Samedit)

https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit


Questions?