Lecture 2: Control Flow Integrity
Last Week...
Last Week…

Attacks

Procedure A
...
call B
...

<table>
<thead>
<tr>
<th>Procedure B</th>
</tr>
</thead>
</table>
| ...
| ...
| Buffer[20]; ...

INTERNAL_SIZE_T prev_size; /* size of prev chunk (if free) */
INTERNAL_SIZE_T size; /* size of chunk */

struct chunk * fd; /* double links -- used only if free */
struct chunk * bw;

Defenses

Procedure A
...
call B
...
exec
...
...

Procedure B
...
...
Buffer[20]; ...

\sh\0"
"\bin
String Ptr
Fake Ret Addr Ptr
Fake Stack Ptr
New Ret Addr Ptr
New Stack Ptr
OverFlow Buffer
B Local Var 2
x86

- Intel Instruction Set Architecture (ISA)
- Introduced 1978, still supported
- As of 2017, most common architecture on servers, PCs, and laptops
- dense instruction set
- variable length instructions
- not word aligned
Return Oriented Programming

\[
\begin{array}{ll}
f7 \ c7 \ 07 \ 00 \ 00 \ 00 & \text{test } 0x00000007, \%edi \\
0f \ 95 \ 45 \ c3 & \text{setnz } -61 (\%ebp) \\
\end{array}
\]

\[
\begin{array}{ll}
c7 \ 07 \ 00 \ 00 \ 00 \ 00 \ 0f & \text{movl } 0x0f0000000, (\%edi) \\
95 \ 45 \ c3 & \text{xchg } \%ebp, \%eax \\
& \text{inc } \%ebp \\
& \text{ret}
\end{array}
\]
Example Gadgets

(a) Load constant gadget

(b) Load from memory gadget
Return Oriented Programming

Return-Oriented Programming is a lot like a ransom note, but instead of cutting out letters from magazines, you are cutting out instructions from text segments.
Return-Oriented Shellcode
Gadget Elimination
Control Flow Integrity
CFI = Insert Monitors
CFI Overhead

![Bar chart showing CFI enforcement overhead for various benchmarks. The chart displays the overhead percentage for benchmarks like bzip2, crafty, eon, gap, gcc, gzip, mcf, parser, twolf, vortex, vpr, and AVG, with crafty showing the highest overhead and bzip2 showing the lowest.](image-url)
Control Flow Guard

- Approximate CFI implementation in Windows 8.1, 10
- Jump is valid if it beginning of function
  - Granularity: 8 bytes
- Check implemented as bitmapa
Control Flow Guard

"Security is lax on this side."
AND NOW FOR SOMETHING COMPLETELY DIFFERENT
What skills will your project need?
Forming a group…

• What skills/experience will you bring to a group?
• What system(s) are you exciting about building?
• How challenging do you want your project to be?
• How often/when are you available to meet?
Milestone 0: Charter

Your charter defines the members of your team and proposes the software system you intend to build. Your charter should include the following information:

- **The members of your team and their contact information.** List the names and NetIDs of your team members.
- **A working name for your system.** You are not committed to this name; it may evolve throughout the semester.
- **A proposal for your system.** Summarize the system you intend to build. You should regard this summary as a starting point; you will have the chance to elaborate in future milestones. Here, you should tell us what will be the most important functionality of your system.
- **Your plan for your weekly status meeting.** We strongly recommend that, as a team, you agree on a weekly meeting time and place (outside of class) that you can both attend to discuss the status of your project. Benefit from our experience: teams that actually do this seem to enjoy more success.

The proposal section of your charter should be about one page long. In this section:

- Provide a very short statement of the core vision or key idea for your system.
- Provide a short bulleted list of the key features of the system.
- Provide a bulleted list of the essential security elements, and a one sentence description of how your system will incorporate each element. Refer to the project overview to make sure your project includes all the required security elements.
- Provide a narrative description of the system you intend to build. Go into enough detail in the body that, if your proposal were given to another team, and that team were never allowed to talk to you, they could still build more or less the system that you have in mind.

**Submission.** Form a group on CMS. As the group, submit a PDF to the Milestone 0 assignment.

**Due:** February 8, 2017 at 11:59pm.