Hacking the Mind

Mike Murray, C.Ht
mmurray@ncircle.com

Frame

“By reading this, you have already given me control over a tiny slice of your mind.”

Frame

Outline

- **The Basics**
  - Hacking and Hypnosis
- **The Exploits**
  - Buffer Overflows and Format String Attacks
  - Data Driven attacks
- **Executing Arbitrary Code**
  - Shellcode and the NOOP Sled
- **Putting it all together**

Hacking and Hypnosis

- **Hacking**
  - Wikipedia definition: a person who *"is able to exploit systems or gain unauthorized access through skills, tactics and detailed knowledge"*
- **Hypnosis**
  - Dave Elman: "*a state of mind in which the critical faculty of the human mind is bypassed, and selective thinking established.*"
- **The Knowledge of Hacking (and Hypnosis)**
  - Know the rules of a given system
  - Know where the edges of the rules/patterns are
  - Know which rules can be bent
  - Know how to creatively bend rules to create positive change

Exploitation

- **Three Main types**
  - Input Handling Overwhelm - the buffer overflow
  - Process / Content Confusion - the format string attack
  - Data Driven Attack - the content / injection attack

- **The Attacks are the same**
  - The mind and the computer each have similar vulnerability
  - Only the mechanisms are different

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

A	A	A	A	A		

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

A	A	A	A	A	A	

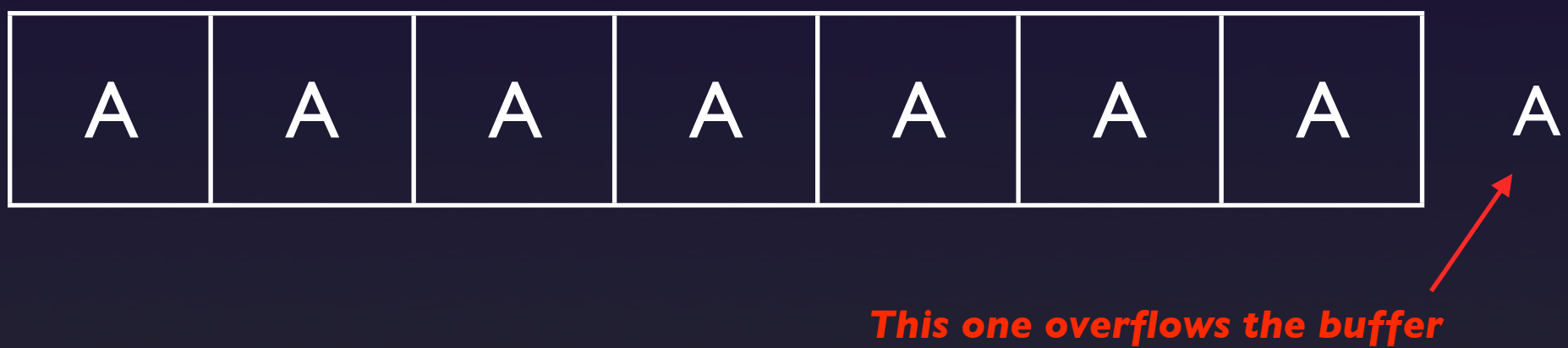
Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

A	A	A	A	A	A	A

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Computer buffer overflows are based on data:**
- **char buf[7];**

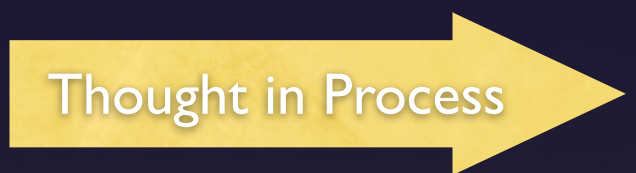


Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Human Buffer Overflows are based on *open loops***
  - A loop is simply any thought or concept
  - Layering loops causes an inability to track consciously

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Human Buffer Overflows are based on *open loops***
  - A loop is simply any thought or concept
  - Layering loops causes an inability to track consciously

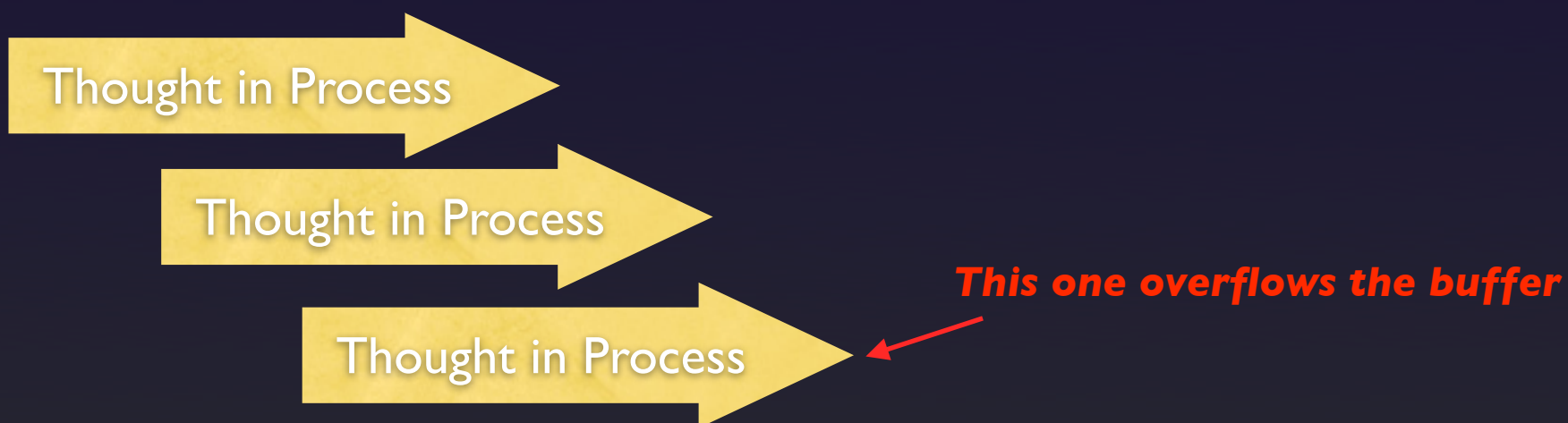


Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Human Buffer Overflows are based on *open loops***
  - A loop is simply any thought or concept
  - Layering loops causes an inability to track consciously

Overflowing Memory

- **The mind has limitations on memory in the same way that a computer does**
- **Human Buffer Overflows are based on *open loops***
  - A loop is simply any thought or concept
  - Layering loops causes an inability to track consciously



Process / Content Confusion

- **The Format String Attack**
  - It is sometimes easy to confuse the computer by making it substitute process for content
  - Format string attack: when a coder forgets to explicitly state their format string in a scanf, for example:

    ```
    char *string;

    scanf(string);  /* should be scanf("%s", string); */
    ```

  - Input such as "blah blah %s blah" would cause the %s to be interpreted as a format string

Process / Content Confusion

- **Linguistic Ambiguity**
  - Hypnotic language patterns often turn on the ability to substitute process for content
  - The conscious mind need not understand the content
- **Ambiguous Content**
  - Syntactic Ambiguity
  - Phonetic Ambiguity

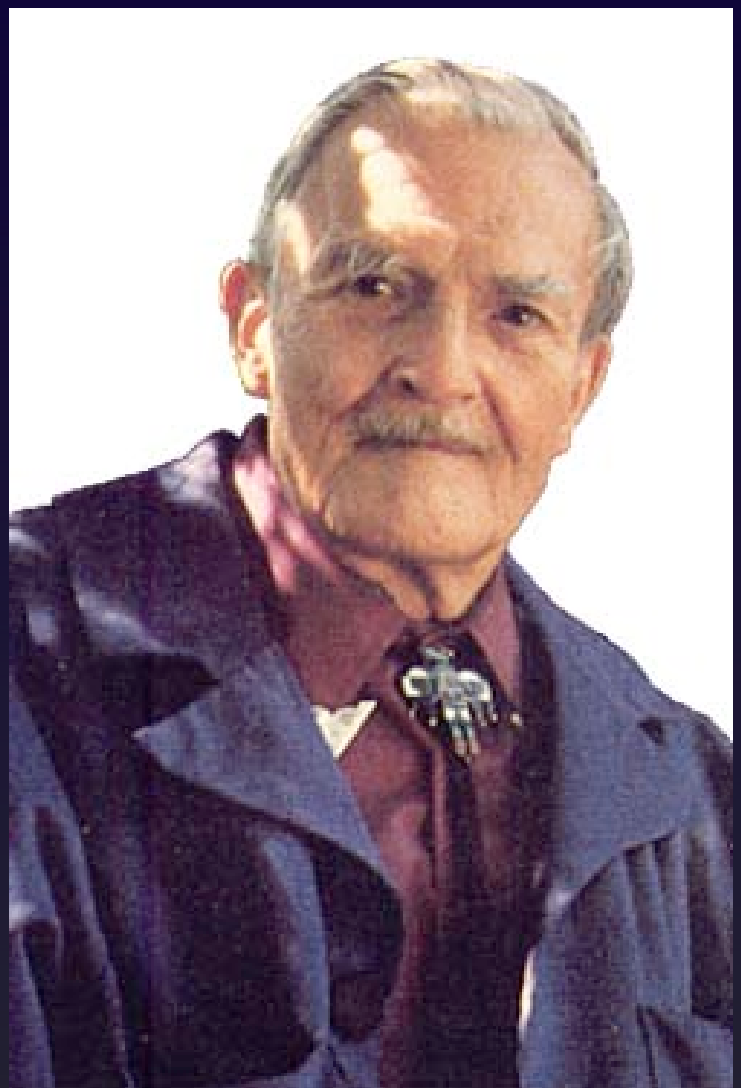
Data / Content Attacks

- **Content can sometimes be an attack**
  - Knowing how content is processed can allow content to change the execution flow
- **The Injection Attack**
  - Knowing that certain structures in content can be interpreted as instructions is important
  - SQL Injection, Cross-site scripting, etc.
- **That reminds me....**

Stories, Metaphors and Patterns

- **The Unconscious mind understands *Patterns***
  - Any content that has a similar structure to a pattern is the equivalent of an instruction about that pattern
  - Example: stories, parables and fairy tales
- **We can structure stories to create the change that we want**
  - A story can be a *"frame"* for an experience - it sets the way that the content within the experience is processed.

Milton Erickson



- **Therapy with Erickson was once described as:**
  - You walked into his office and sat down. Then, Milton told you a story and you found yourself changing.
  - Milton created frames in which change happened automatically

Executing Arbitrary Code

- **Moving past the exploit**
  - The point is to actually DO something
  - Executing your own code
- **Two Pieces**
  - NOOP Sled - allowing the system to run harmless instructions to deepen the exploit into fertile memory space
  - Shellcode - crafting actual instructions that can be executed in order to create the change you're looking for

NOOP Sled

- **Going deeper into the overflow**
  - NOOPs are inserted into the exploit to ensure that shellcode is able to run
- **Going deeper into the unconscious mind**
  - Giving the unconscious permission to trust the process
- **Being *"Artfully Vague"***
  - Using language that corresponds to any human experience
  - Giving permission to move forward in the process

Actually Running Instructions

- **The language of the unconscious mind is indirect**
  - Erickson believed that the unconscious would not respond to direct instructions
  - It is better to give opportunities than giving commands

- **The most powerful pattern in the world**
  - What if there was a language pattern that could ensure that anyone who heard it would execute the program that you chose?
  - There is...

The Importance of the Question

- **The question *can not* be avoided by the unconscious mind**
  - If you ask a question, it will be answered
  - This doesn't have to be conscious

- **Knowing how to use questions is the key of making change**
  - Questions can ensure that your content gets processed, can't they?

Closing the Frame

Thanks

Mike Murray, C.Ht
mmurray@ncircle.com || mmurray@episteme.ca