Trojan Source

Invisible Vulnerabilities

Nicholas Boucher
University of Cambridge

Ross Anderson
Universities of Cambridge & Edinburgh
Some Vulnerabilities are Invisible
Encoding

RTL

Reset

Rendering

c b a
Source Code?
Comments + String Literals
The Vulnerability

1. **Control characters** can override text direction.

2. This can **modify display order**.

3. They can be **placed into comments and strings**.

⇒ Evil program A to be anagrammed into benign program B.
The Vulnerability

```c
#include <stdio.h>
#include <stdbool.h>

int main() {
    bool isAdmin = false;
    /* begin admins only */
    if (isAdmin) {
        printf("You are an admin.\n");
    /* end admins only */
    return 0;
}
```

The Vulnerability

/* if (isAdmin) { begin admins only */
The Vulnerability

```c
#include <stdio.h>
#include <stdbool.h>

int main() {
    bool isAdmin = false;
    /* begin admins only */ if (isAdmin) {
        printf("You are an admin.\n");
    /* end admins only */
    
    return 0;
}
```

```bash
$> clang program.c && ./a.out
You are an admin.
$> |
```
Supply Chain Attack
Coordinated Disclosure
```c
#include <stdio.h>
#include <stdbool.h>

int main() {
    bool isAdmin = false;
    /* U+202E */
    if (isAdmin) begin admins only */
    printf("You are an admin.\n");
    /* end admins only */
    return 0;
}
```
```c
#include <stdio.h>
#include <stdbool.h>

int main() {
    bool isAdmin = false;
    /* begin admins only */
    printf("You are an admin.\n");
    /* end admins only */
    return 0;
}
```
warning: unicode codepoint changing visible direction of text present in literal
   src/test/ui/parser/unicode-control-codepoints.rs:24:26
24 |     println!("{?: }", "/\u{2066} if isAdmin \u{2066} begin admins only ");
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
   \\
   this comment contains invisible unicode text flow control codepoints
   
   = note: `#[force-warn(text_direction_codepoint_in_literal)]` on by default
   = note: these kind of unicode codepoints change the way text flows on applications that support them, but can cause
   = help: if their presence wasn't intentional, you can remove them
   help: if you want to keep them but make them visible in your source code, you can escape them
24 |     println!("{?: } \u{2066} if isAdmin \u{2066} \u{2066} begin admins only ");
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
Unicode has convened a group of experts in programming languages, tooling, and security to provide guidance and recommendations on how to better handle international text in source code, as well as providing code to help implementations.
See paper for...

- Attack Generation
- Attack Detection
- Attack Variants
- CVE Details
- Compiler vs Editor vs Repo
- GitHub Ecosystem Scanning
- Coordinated Disclosure Details
- Industry Response
- Defenses

... and more
It’s not just source code

- **LLMs**  
  *Bad Characters: Imperceptible NLP Attacks*  
  *(S&P 2022)*

- **Search Engines**  
  *Boosting Big Brother: Attacking Search Engines with Encodings*  
  *(RAID 2023)*

- **Coordinated Disclosure**  
  *Talking Trojan: Analyzing an Industry-Wide Disclosure*  
  *(SCORED 2022)*
More Info

https://trojansource.codes