Secure Software Design and Analysis

—

Tyler Apostolico, Roberto Hanna, Will Rembish

CERT rules for C++

- CERT is a division of the software institute at CMU - one of the most well-known CS institutions in the US.
- Effort to get universal coding standards for various languages to solve modern cyber security issues
- Deal with various coding practices from proper variable initialization to securely allocating memory
- There are hundreds of CERT rules

CERT (Cont.)

Each CERT rule has:

- Likelihood
- Severity
- Remediation Cost
- Priority

Even on current rules, many disagree on these additional factors

- The CERT website has a forum where users comment on their view of the rules and possible overlaps of other rules.

Where do we apply secure software and CERT rules?

Everywhere.

The Projects

Our Projects

Approximately two weeks of time for each of them

- Markovian Tweet Generation
- Minesweeper
- Secure Email Database
- Polynomial Multiplier/Adder
- Followed various CERT rules

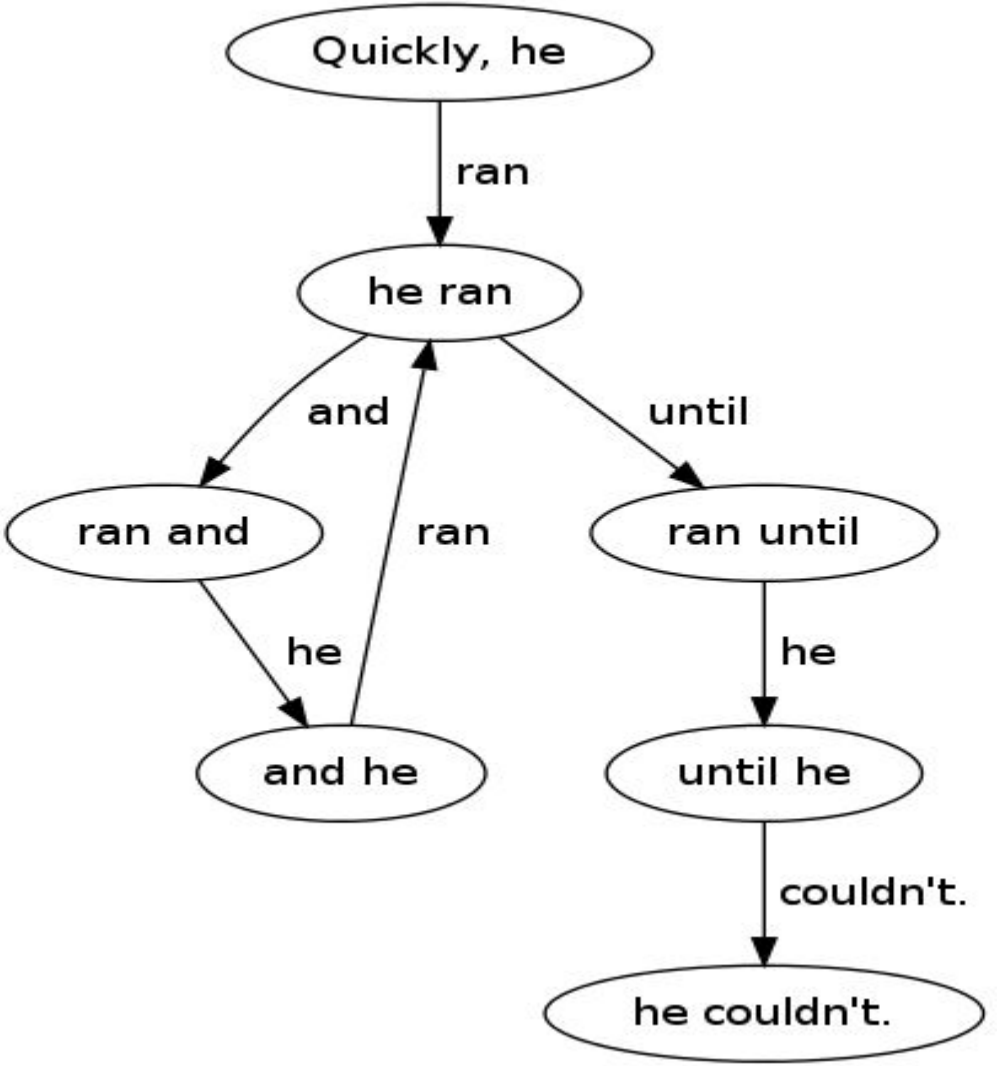
- All done in C++

Markovian Tweets

1. Takes in an input txt file of words. Prints tweet in output file.

2. Builds a map of nested vectors with two word keys, each key used to predict likely next word in the tweet. Every time a word is added, change the key.

3. Limited to 140 character tweet-like generation of any person of your choosing - Shakespeare, Obama, Anyone.



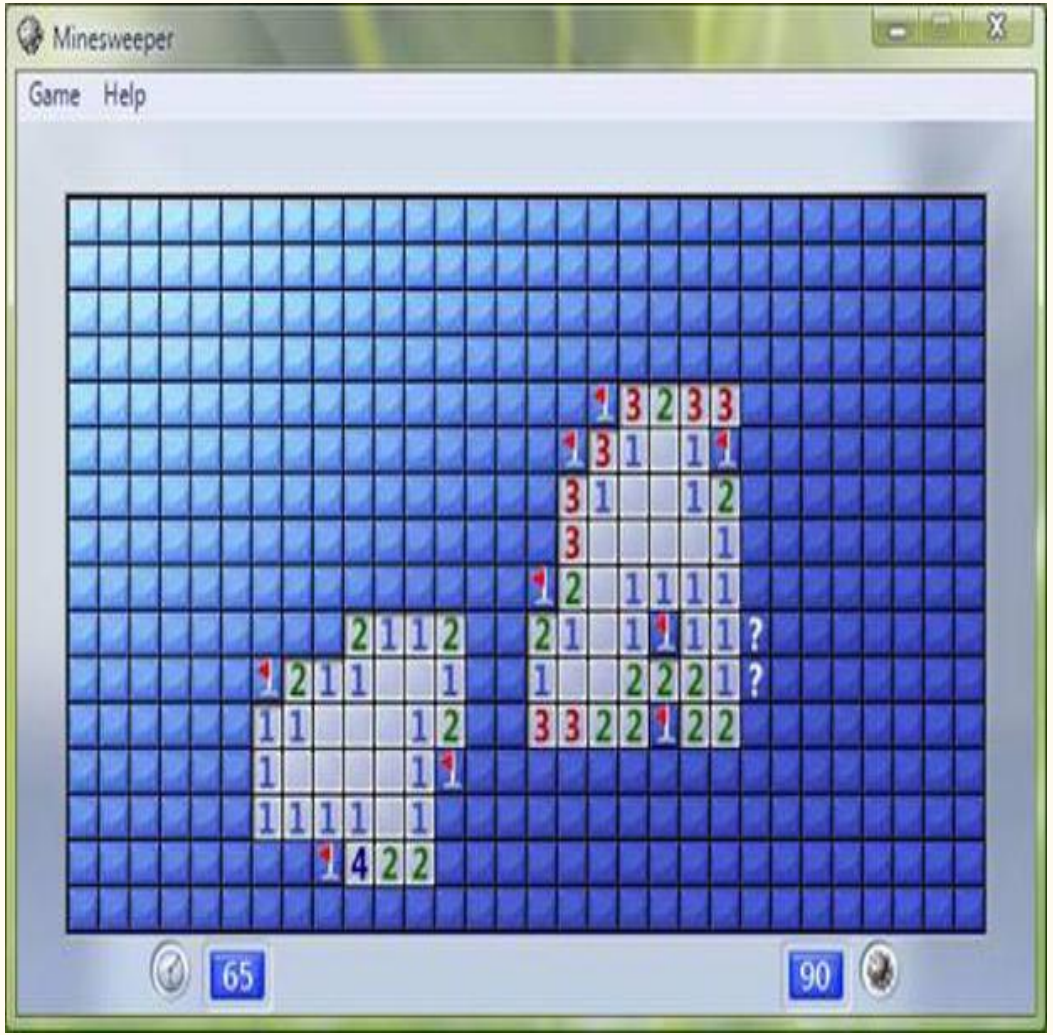
Minesweeper

1. This version of minesweeper dealt with heavy user input and output through the command line.

2. Classic game to try to uncover all of the bombs in a grid of cells.

3. CERT rules primarily dealt with arrays management and using proper expressions.

4. Based on 2D vector of Cells.



Polynomial Calculator

1. Takes in two polynomials from input files, and prints the answers in an output file.
2. Multiplies (distribution method) and adds polynomials of any degree.
3. CERT rules primarily dealt with memory management and proper handling of characters and strings.

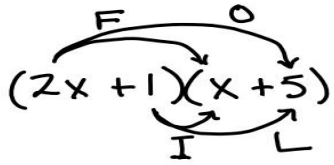
Polynomial Multiplication

Methods

1. F.O.I.L. (Binomials only)
2. Distribute
3. Special Rules

F.O.I.L. (First, Outter, Inner, Last)

Example $(2x+1)(x+5)$



$(2x+1)(x+5) = 2x(x) + 2x(5) + 1(x) + (1)(5)$

$= 2x^2 + 10x + 1x + 5$

Answer $= 2x^2 + 11x + 5$

Distribute Method

Example $(x-5)(3x^2+2x-4)$

$(x-5)(3x^2+2x-4) = 3x^3 + 2x^2 - 4x$

$(x-5)(3x^2+2x-4) = -15x^2 - 10x + 20$

add like terms

Answer $= 3x^3 - 13x^2 - 14x + 20$

Adding Polynomials

Polynomial $(5x^2 + 3x + 2)$ + Polynomial $(-3x^2 + 4x + 5)$

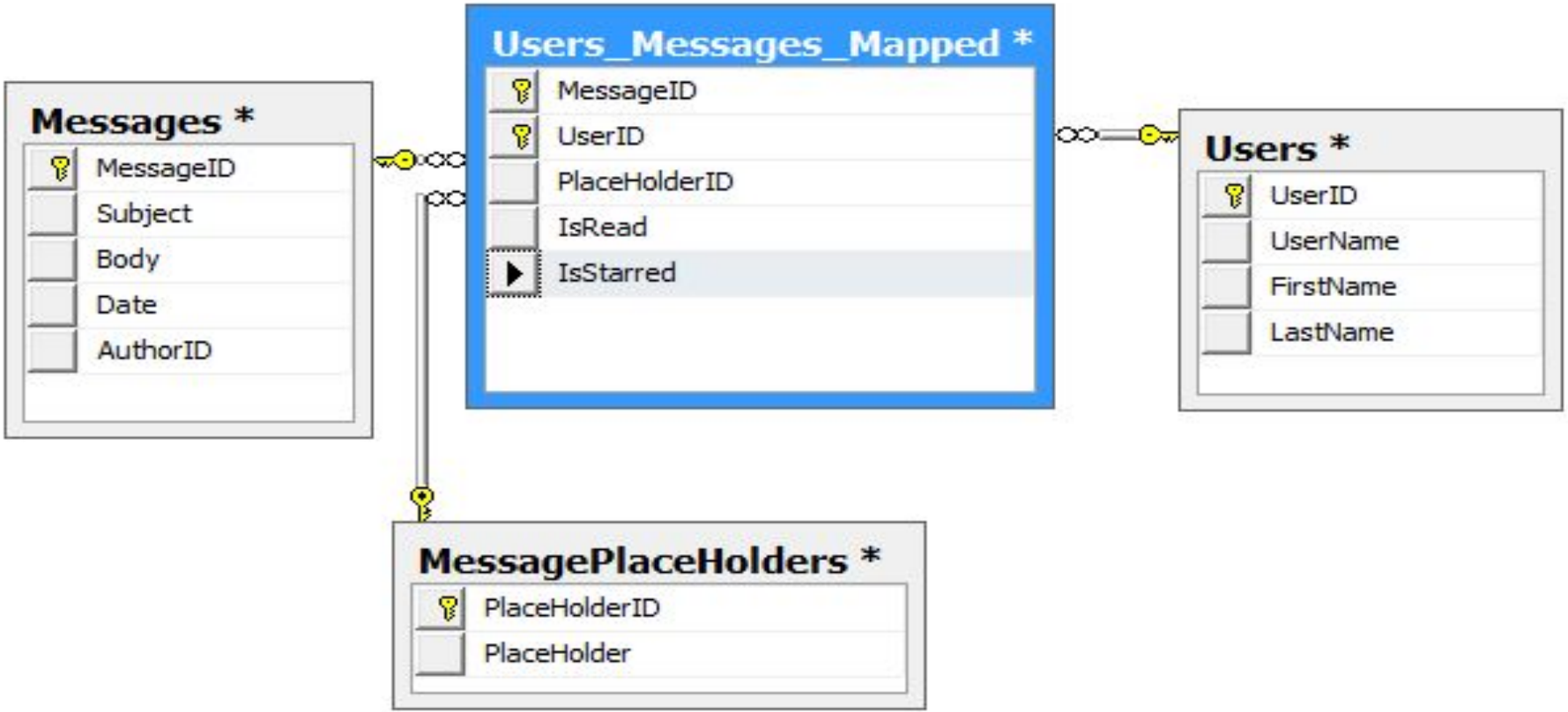
↓ ↓

COMBINE LIK

$5x^2 + 3x + 2 - 3x^2 + 4x + 5$

Secure Email Database

1. Application of sqlite in C++ to create an encrypted database to store, write, and access messages.
2. Usernames and passwords were all encrypted and decrypted when necessary to be secure.
3. CERT rules that applied relied heavily on getting proper inputs and dealing with user input errors through exception handling.


Users_Messages_Mapped *
MessageID
UserID
PlaceHolderID
IsRead
IsStarred
Messages *
MessageID
Subject
Body
Date
AuthorID
Users *
UserID
UserName
FirstName
LastName
MessagePlaceHolders *
PlaceHolderID
PlaceHolder

Switching Code

- After coding our projects, we exchanged projects with another group and checked for further security.
- Analysis of further (different) CERT rules.
- Displayed the “two way street” of hacking software versus security of software.

Takeaways from projects

Secure software design is ever-changing as hackers adapt to our practices.

CERT rules can only go so far in securing software.

All global level applications of software need to be secure to protect company and user information.

Questions?