THERE AND BACK AGAIN

BRIAN CHESS

SEPTEMBER 2013


NATIONAL SECURITY
AGENCY

Fred

Joe

Sam

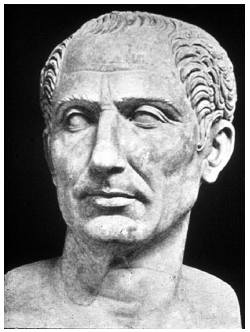
Fred

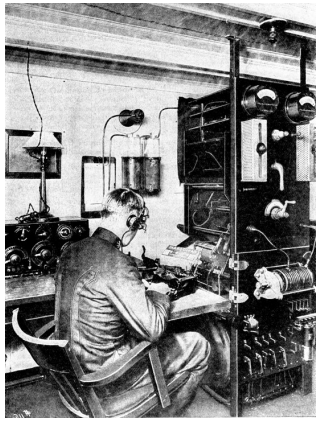
Joe

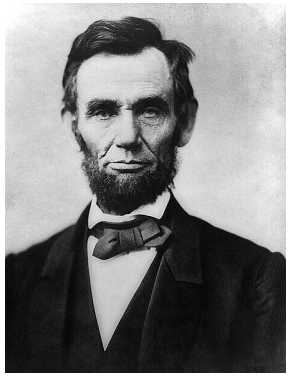
Sam


NATIONAL SECURITY
AGENCY

A BRIEF HISTORY OF COMMUNICATIONS SECURITY







COMPUTER SECURITY

THE PROGRAMMER

"Programming is hard"

Donald Knuth

- Programmers not historically responsible for security.
- Programmers already have one hard job to do.

DEFENSIVE PROGRAMMING IS NOT ENOUGH

Defensive programming: "Write the program to cope with small disasters." [Kernighan and Plauger]

A C function with no error checking:

```
void printMsg(FILE* file, char* msg) {
  fprintf(file, msg);
}
```

Crashes when file or msg is null.

DEFENSIVE PROGRAMMING IS NOT ENOUGH

Error checking added:

```
void printMsg(FILE* file, char* msg) {
  if (file == NULL) {
    logError("attempt to print to null file");
  } else if (msg == NULL) {
    logError("attempt to print null message");
  } else {
    fprintf(file, msg);
  }
}
```

No more crashes. Fixed?
Hint: AAA1_%08x.%08x.%08x.%08x.%08x.%n

THIS IS ENOUGH

Must also defend against *format string attacks*:

```
void printMsg(FILE* file, char* msg) {
  if (file == NULL) {
    logError("attempt to print to null file");
  } else if (msg == NULL) {
    logError("attempt to print null message");
  } else {
    fprintf(file, "%.128s", msg);
  }
}
```

SOFTWARE QUALITY VS. SOFTWARE SECURITY

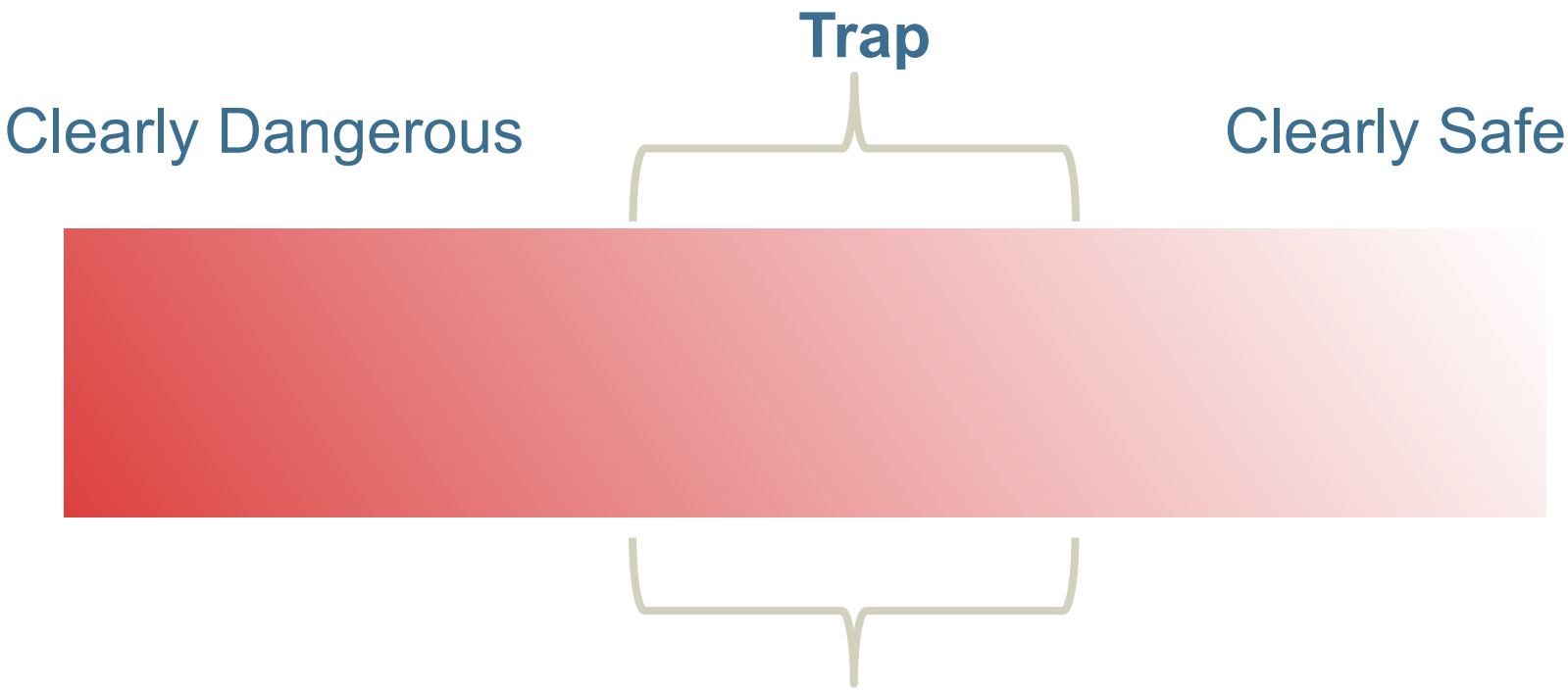
QUALITY

- Cannot be bolted on
- Must be built in
- Does the program do what it's supposed to do?
- Will the users be happy?
- Are common cases smooth and easy?
- Will people pay for it?

SECURITY

- Cannot be bolted on
- Must be built in
- Does the program have “bonus” features?
- Will the attackers get what they want?
- Are there corner cases we haven't considered?
- What do we stand to lose?

THE EXPLOITABILITY TRAP



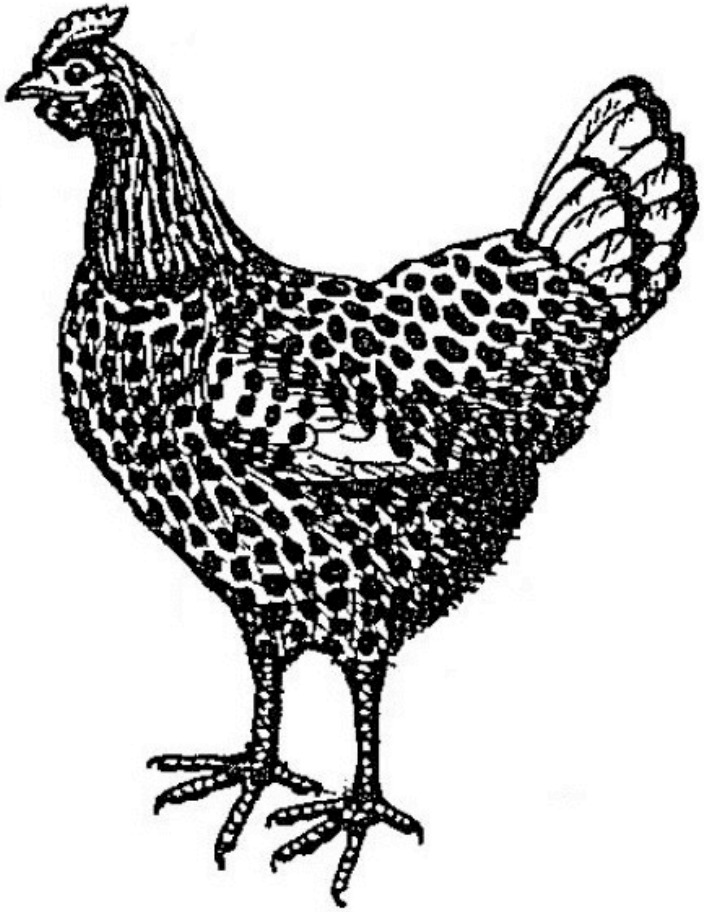
CITI IPHONE INFO LEAK

BERTRAND RUSSELL'S CHICKEN

Food

Shelter

Companions



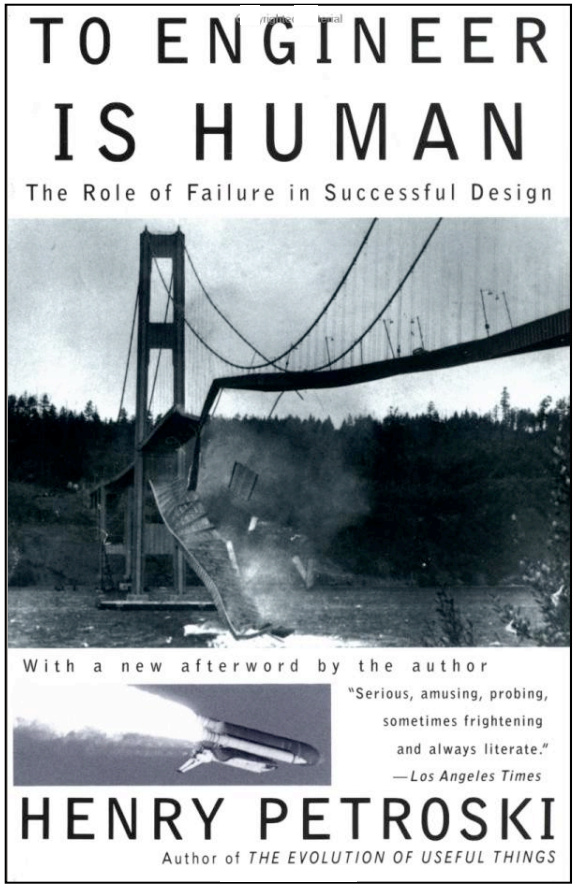
Food

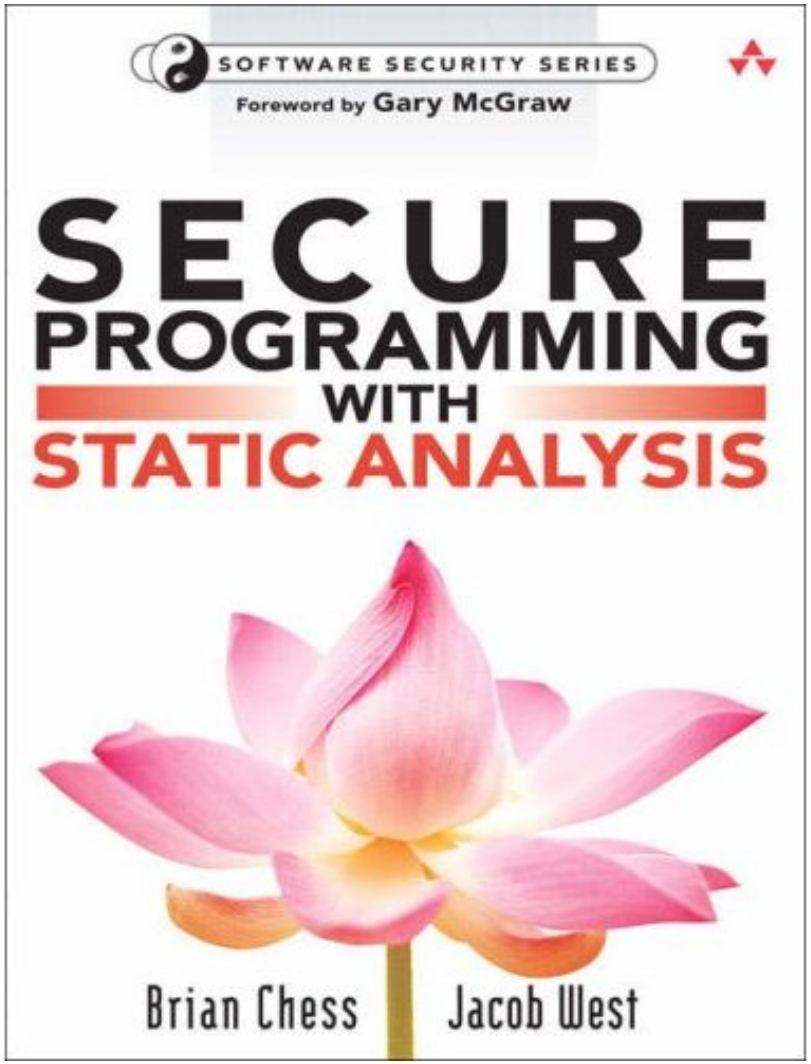
Shelter

Companions

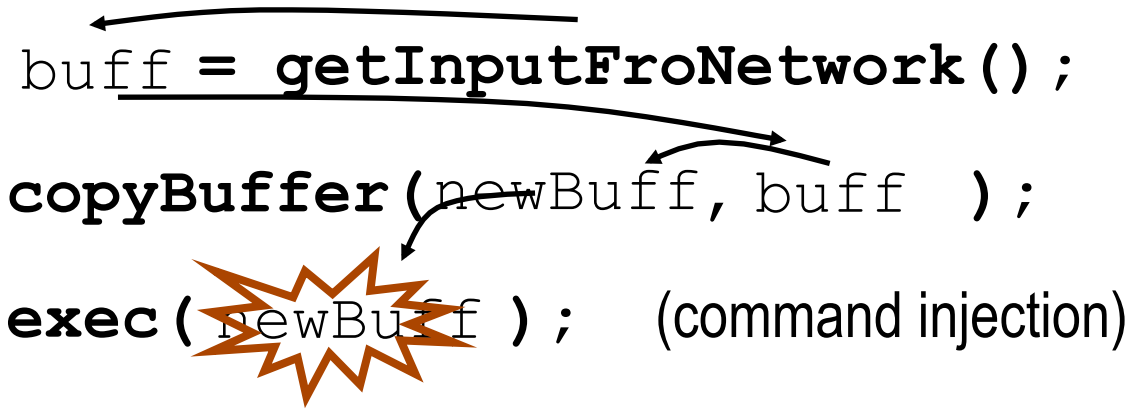
Success is foreseeing failure.

– Henry Petroski




SOFTWARE SECURITY SERIES
Foreword by Gary McGraw
SECURE
PROGRAMMING
WITH
STATIC ANALYSIS
Brian Chess
Jacob West

STATIC ANALYSIS = GOOD




Husqvarna
137

MEASURING PROCESS

Building Security In Maturity Model (BSIMM)

http://www.bsi-mm.com

THERE AND BACK AGAIN

BRIAN CHESS

SEPTEMBER 2013