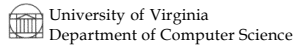


Outrageous Opinion

# Securing Bits with Atoms

(and Vices with Verses)

David Evans  
evans@cs.virginia.edu  
<http://www.cs.virginia.edu/evans>



## Non-Outrageous Opinion #1

Trustworthy software is hard  
...and its not getting any easier

- Software is getting more complex faster than software engineering methods are improving
- Humans aren't getting any smarter

6 January 2003

DIMACS

2

## Non-Outrageous Opinion #2

Most physical things are very trustworthy

- Bridges rarely fall down
- 13 million commercial airline takeoffs/landings in 2002 with 0 fatalities! (CNN.com, 3 Jan)
  - Hmm...there was a lot of software involved too, maybe opinion #1 needs reconsideration!

6 January 2003

DIMACS

3

## Why Software is Harder

- | Hardware   | Software  |
|--|---|
| • Continuous <ul style="list-style-type: none"><li>– Adjacent states are similar</li></ul>                                 | • Discrete <ul style="list-style-type: none"><li>– Adjacent states can be completely different</li></ul>                              |
| • Inertia <ul style="list-style-type: none"><li>– Changes require force</li><li>– Big changes require more force</li></ul> | • Weightless <ul style="list-style-type: none"><li>– No force required</li><li>– Changing a single bit can break everything</li></ul> |
| • Visible and Touchable <ul style="list-style-type: none"><li>– Easy to see tampering</li></ul>                            | • Invisible and Odorless <ul style="list-style-type: none"><li>– Hard to smell tampering</li></ul>                                    |

6 January 2003

DIMACS

4

## Can we make software more like hardware?

- Yes! Computing is becoming embedded in physical stuff
- Computing elements live in physical worlds – are beginning to interact with them directly
- ...but mostly indirect: sensors and actuators attached to computing devices, but programs do not integrate computing and physical environment

6 January 2003

DIMACS

5

## Tip-of-Iceberg Examples

- Location-Limited Channels [Stajano & Anderson 99 (“Resurrecting Duckling”), [Balfanz, et. al., NDSS 02]
  - Exploit physical properties of communication medium for authentication and confidentiality
- Physical One-Way Functions [Gershenfeld & Pappu, 02]
- Amorphous Computing [Abel, et. al., CACM00], Cell-Based Computing [George & Evans, WOSS 02]
  - Program global behaviors using local interactions

6 January 2003

DIMACS

6

## Motto

The Future of Software is  
“Shardware”  
(not “Shaftware”)

6 January 2003

DIMACS

7

## Any questions?

David Evans  
evans@cs.virginia.edu  
<http://www.cs.virginia.edu/evans>



University of Virginia  
Department of Computer Science

6 January 2003

DIMACS

8