Where to Now?

Steven M. Bellovin
http://www.cs.columbia.edu/~smb
Columbia University

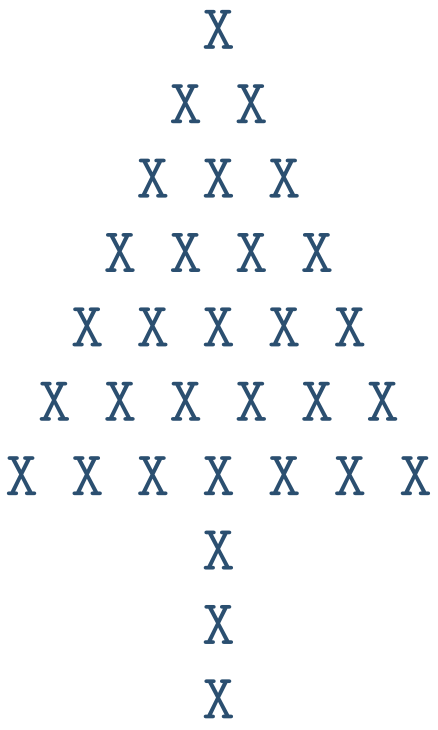
December 12, 2006

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

The Past

19 Years Ago, This Weekend

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future



A very happy Christmas and my best wishes for the next year. Let this run and enjoy yourself. Browsing this file is no fun at all.
Just type Christmas.

The IBM Christmas Card "Virus"

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

- A simple executable script
- When invoked, it displayed an animated Christmas tree
- It also scanned the user's alias file for the addresses of contacts, and sent out a copy of itself to each one
- Sound familiar?

The Internet Worm

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

- 11 months later, it happened again
- A worm was unleashed that spread by many different mechanisms, including password-guessing and buggy software
- Multi-protocol, multi-platform — took out *lots* of machines

What Have We Learned?

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

What Would Have Stopped Those?

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

Human Nature

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

- There are no patches available for *H. sapiens* 1.0

Human Nature

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

- There are no patches available for *H. sapiens* 1.0
- The release date for 2.0 has not been announced

Human Nature

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

- There are no patches available for *H. sapiens* 1.0
- The release date for 2.0 has not been announced
- There are no betas in sight

Security Standards

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

Me "I just reread the Orange Book; nothing in it would have prevented the worm.

Security Standards

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

Me "I just reread the Orange Book; nothing in it would have prevented the worm.

Him "No, that's not so; a B2 system would have stopped it."

Security Standards

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

Me "I just reread the Orange Book; nothing in it would have prevented the worm.

Him "No, that's not so; a B2 system would have stopped it."

Me "How so?"

Security Standards

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

Me "I just reread the Orange Book; nothing in it would have prevented the worm.

Him "No, that's not so; a B2 system would have stopped it."

Me "How so?"

Him "B2 requires a thorough search for bugs."

Security Standards

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

Me "I just reread the Orange Book; nothing in it would have prevented the worm.

Him "No, that's not so; a B2 system would have stopped it."

Me "How so?"

Him "B2 requires a thorough search for bugs."

Me "Oh. . ."

These Weren't New

The Past
19 Years Ago, This Weekend
The IBM Christmas Card "Virus"
The Internet Worm
What Have We Learned?
What Would Have Stopped Those?
Human Nature
Security Standards
These Weren't New
The Present
The Future

- My friends and I discussed "rabbit jobs" circa 1972, and we knew we weren't inventing them
- I saw my first fake login prompt (not "login screen"!) in 1969
- Hoare warned about buffer overflows as a security problem in his 1980 Turing Award lecture

The Past
The Present
Progress?
Systems Are Somewhat Better
Fudd's First Law of Opposition
The Future

The Present

Progress?

The Past
The Present
Progress?
Systems Are Somewhat Better
Fudd's First Law of Opposition
The Future

- We still see phishing, come-and-get-it attacks, and pump-and-dump spam
- We still see buffer overflows
- The only reason we don't see more "bring down the Net" worms is because they're bad for (evil) business
- Have we made progress?

Systems Are Somewhat Better

The Past
The Present
Progress?
Systems Are Somewhat Better
Fudd's First Law of Opposition
The Future

- I'm no longer surprised to see a computer that's been up for a year or more
- We no longer reboot our computers daily because they really need it; even ordinary desktops can (usually) survive overnight
- But it doesn't seem to take much of a push to knock things over

Fudd's First Law of Opposition

The Past
The Present
Progress?
Systems Are Somewhat Better
Fudd's First Law of Opposition
The Future

"Push something hard enough and it will fall over."

Firesign Theater, 1971

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

The Future

Where Now?

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- We're not going to fix human nature
- We're not going to abolish buggy software
- Is there a solution?

CS@CU

Where Now?

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- We're not going to fix human nature
- We're not going to abolish buggy software
- Is there a solution?
- Not a perfect one, but we can (probably) achieve "good enough"

High-Quality Software

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- We've been able to produce high-quality software when people cared enough (and paid enough)
- Yes, there have been plenty of problems with phone switches, avionics, and the like, but on the whole such software has a much better track record
- What does it take?

How is it Done?

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- Disciplined software engineering
- We must understand our goals
  $\Rightarrow$That may be "keep flying" or "keep the switch up"
- Understand that people are part of the system
- The software architecture must be aimed first at those goals

The Human Element

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- Human beings are an essential part of our computer systems
- We must design our systems to be resilient in the face of human error
- We must also design them to minimize such errors

Words of Wisdom

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

"If we assume that the people who use technology are stupid ('Bubbas') then we will continue to design poorly conceived equipment, procedures, and software, thus leading to more and more accidents, all of which can be blamed upon the hapless users rather than the root cause – ill-conceived software, ill-conceived procedural requirements, ill-conceived business practices, and ill-conceived design in general."

Don Norman, *Risks Digest 23.07*, 2003

Architecture

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- We are never going to have absolutely-correct programs
- We can design systems to protect what really counts
- This requires a change in architecture
- Coding practices, no matter how good, won't help

Caveats

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

Caveats

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- "You can't make systems foolproof because fools are so smart"

Caveats

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- "You can't make systems foolproof because fools are so smart"
- You have to *know* what really counts

Caveats

The Past
The Present
The Future
Where Now?
High-Quality Software
How is it Done?
The Human Element
Words of Wisdom
Architecture
Caveats

- "You can't make systems foolproof because fools are so smart"
- You have to *know* what really counts
- You'll still get it wrong sometimes — but less often