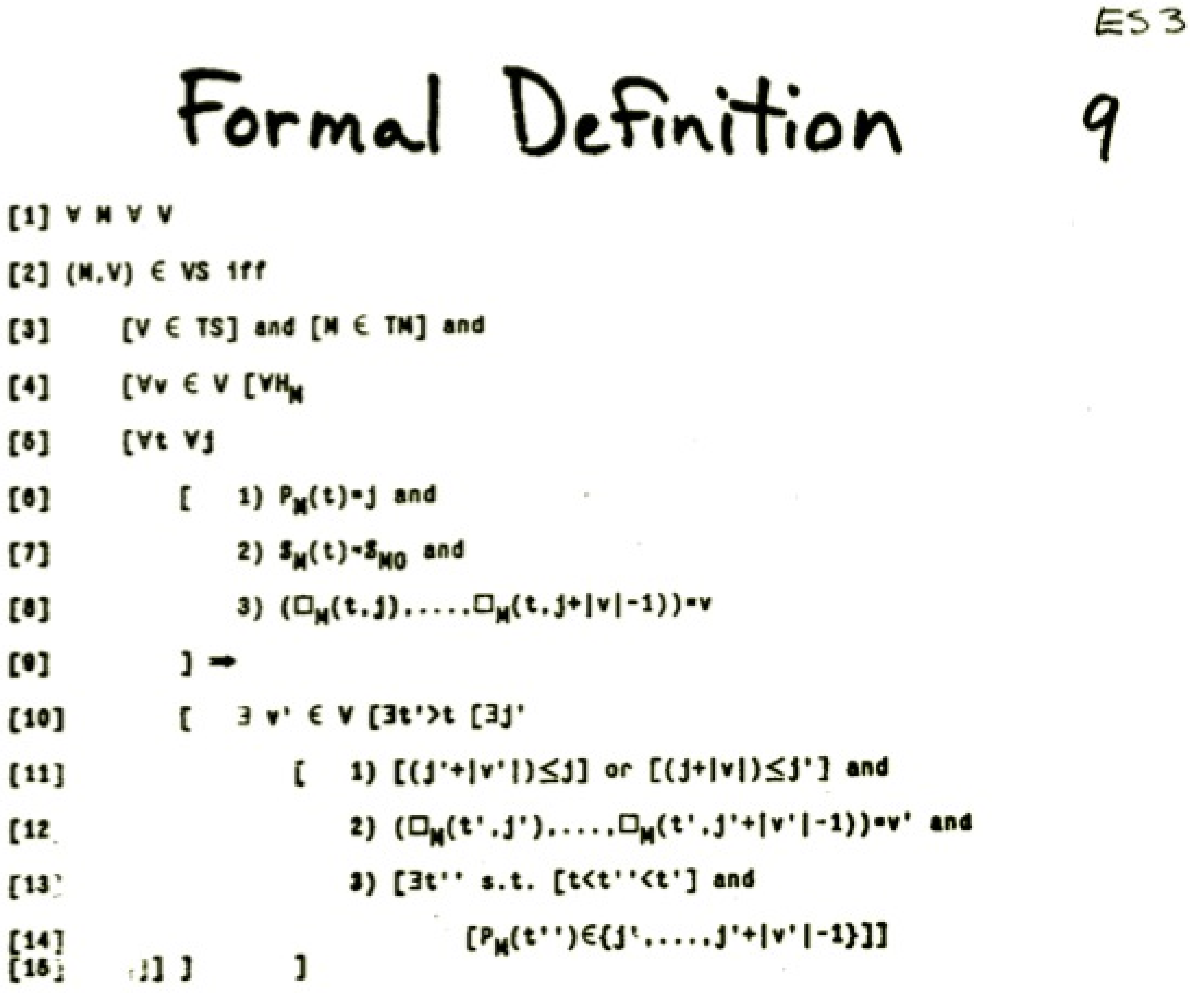
Computer Viruses
Then – Now – Then Again

May 11, 2009

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

I'd like to start with a ...



ES3

Formal Definition 9

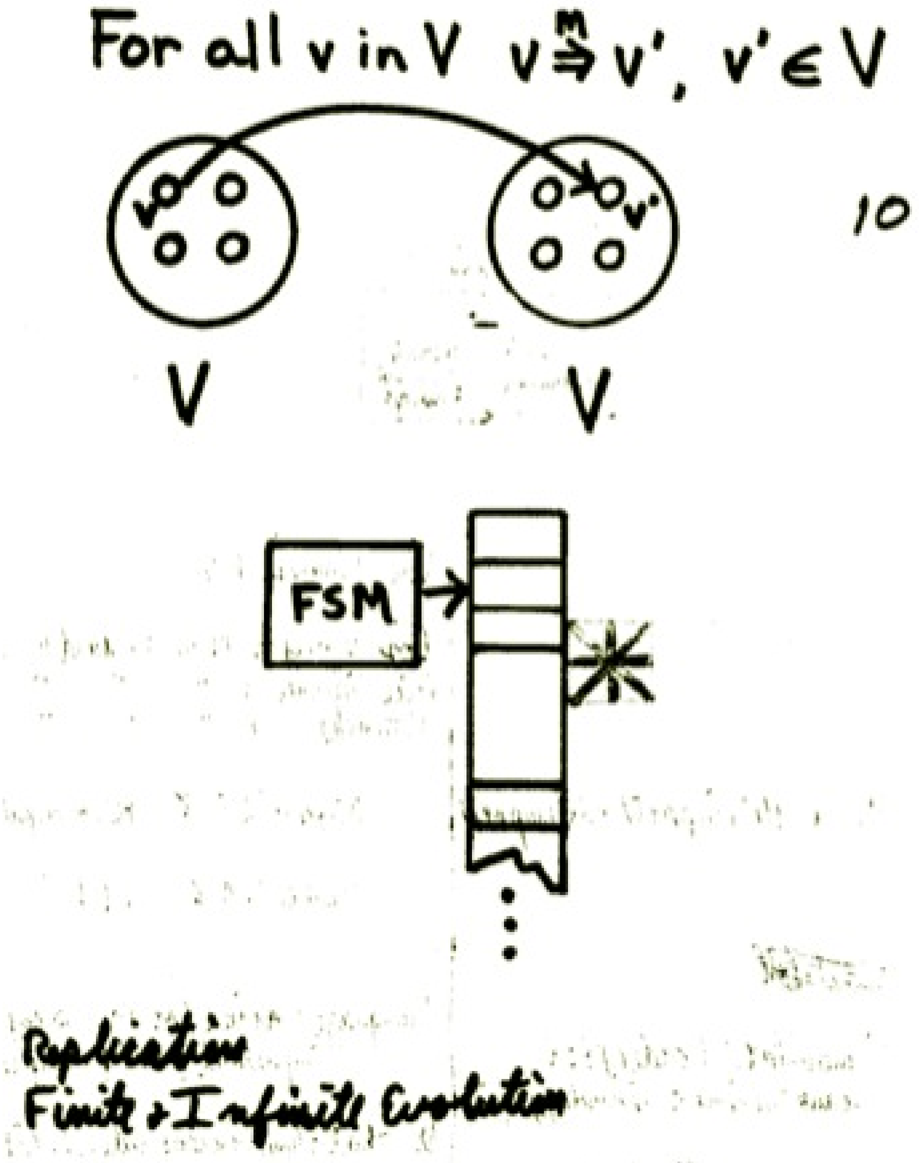
```
[1] ∀ M ∀ V
[2] (M,V) ∈ VS iff
[3]      [V ∈ TS] and [M ∈ TM] and
[4]      [∀v ∈ V [∀H_M
[5]      [∀t ∀j
[6]          [   1) P_M(t)=j and
[7]              2) $_M(t)=$_M0 and
[8]              3) (□_M(t,j),....,□_M(t,j+|v|-1))=v
[9]          ] ⇒
[10]         [   ∃ v' ∈ V [∃t'>t [∃j'
[11]                 [   1) [(j'+|v'|)≤j] or [(j+|v|)≤j'] and
[12                      2) (□_M(t',j'),....,□_M(t',j'+|v'|-1))=v' and
[13]                     3) [∃t'' s.t. [t<t''<t'] and
[14]                           [P_M(t'')∈{j',....,j'+|v'|-1}]]
[15]     :]] ]       ]
```

Outline

- The past...
- Simmering...
- Today
- Then what?

November 3, 1983

- Sitting in Len Adleman's computer security class at USC
- I had a moment of clarity
  - Assume a Trojan horse in the $PATH
  - Suppose it replicates into user programs?
  - Wait 3 seconds...
  - Game over!

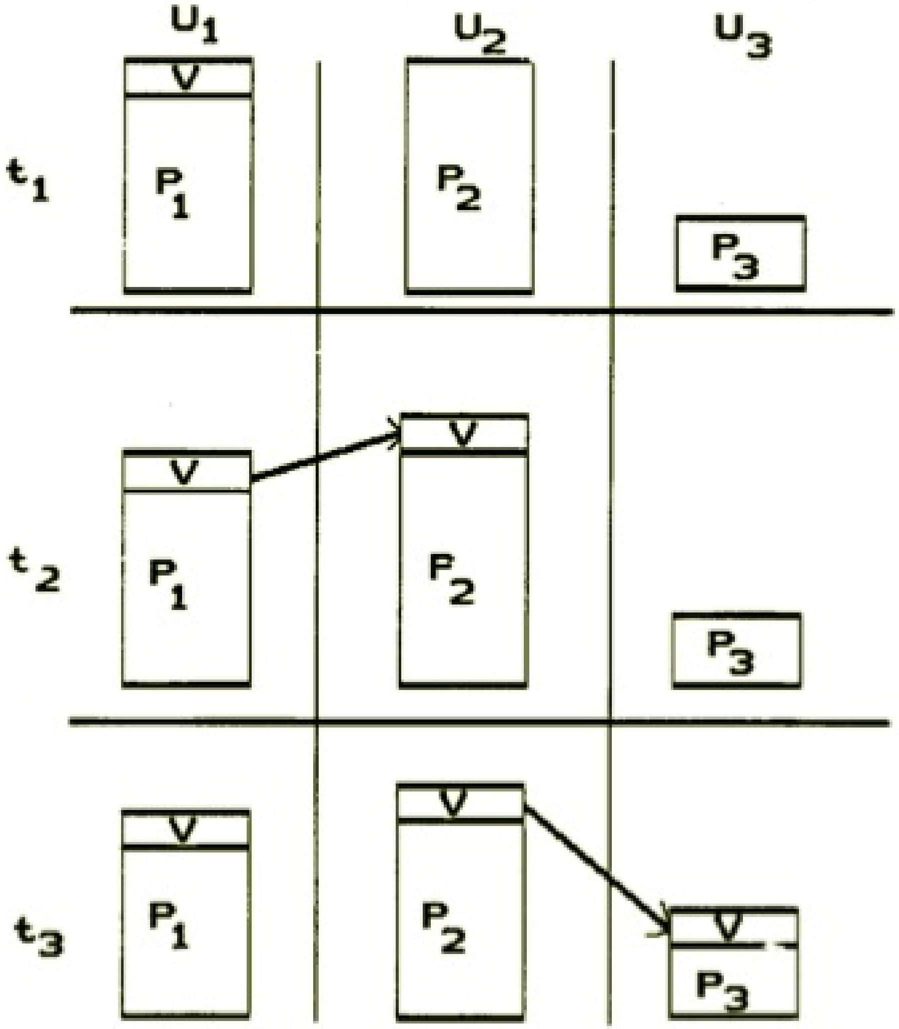

For all v in V $v \overset{m}{\Rightarrow} v'$, $v' \in V$
v
v'
10
V
V
FSM
Replication
Finite → Infinite evolution

1983-11-04

- First experiments
- Timesharing system
- ~35 users
- No security flaws exploited
- Time to root...
  - Min 5 sec
  - Avg 30 min
  - Max 1 hour
- Uh oh!!!

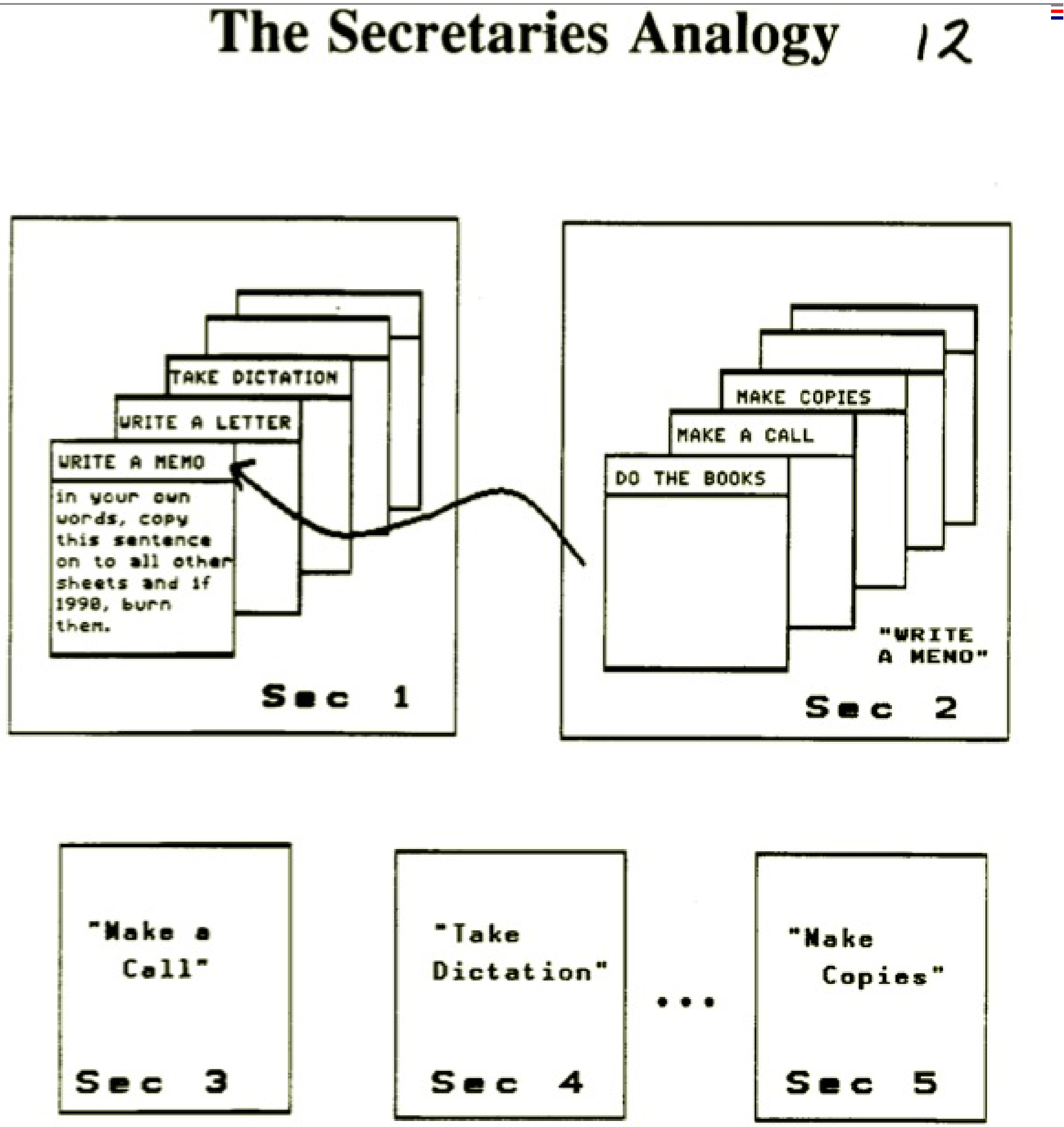
Working Definition of a Virus //

A program that can "infect" other programs by modifying them to include a possibly evolved copy of itself.



Try to explain it...

- How I explained it t
  the department
  secretaries
- Hence...
  - The secretaries
    analogy
- This was needed til
  about 1989...
- In the computer
  science community

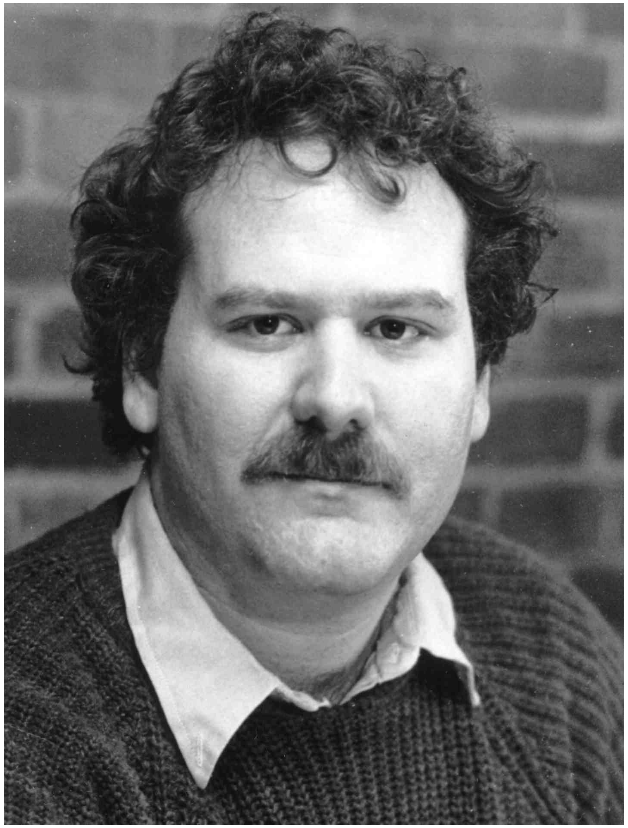


in your own words, copy this sentence on to all other sheets and if 1998, burn them.

1984 IFIP TC11 in Canada

- The first presentation of “Computer Viruses – Theory and Experiments”
  - I was scheduled to give: “Algorithmic authentication of identification”
  - Herald Highland told me to go ahead and substitute this talk
- After the talk I was approached by a State Department official who said:
  - If you would have told us you were presenting this, we wouldn't have let you.
- And I said...
  - “That's why I didn't tell you”

1984 – just after IFIP



- I show up at the border to the US
- Wearing genes and a tee shirt
- Carrying only a backpack
  - The boarder guard is all friendly and happy – all smiles...
  - He types in my passport number
  - His face turns ashen gray!!!
  - He searches my backpack very thoroughly – looking at every sheet of paper – but ignoring my floppy disks!!!

1984 – the NCSC conference

- “Computer Viruses – Theory and Experiments”
    - The 2nd time – at the NSA annual conference
    - I show how TCSEC computers can be infiltrated with viruses
    - I show how covert channels can leak classified
    - But the TCSEC is just about to be approved
- The TCSEC (Orange book) is approved with one known unaddressed flaw...
    - The NSA is less than thrilled with me...

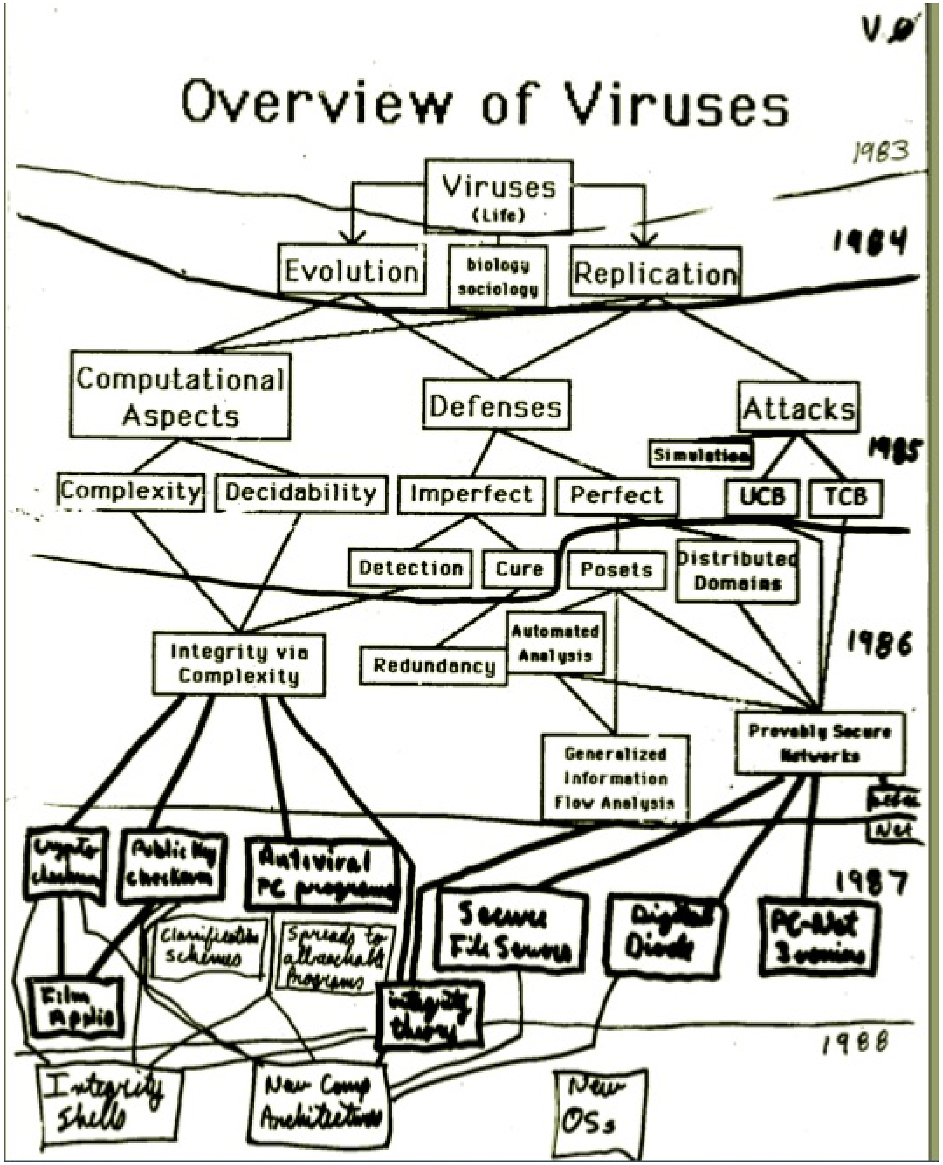
1984-8 Research & rejection

- 1986 – finished dissertation (Lehigh)
  - “Computer Viruses” - the Red book
- 1987 – went to U of Cincinnati
  - NSF rejected research proposal
  - Evaluators said the theoretical virus thing could never work in a real computer system
- 1988 – Headed “The Radon Project”
  - You have to earn a living as well as doing research
- Average 4+ refereed journal articles/y

THE RADON PROJECT
THE RADON PROJECT
RADON TEST KIT FOR THE HOME AND WORKPLACE
Made in the USA
Safe!
Easy!
EPA LISTED LABORATORY
THE RADON PROJECT
Certified by The Department of Environmental Resources
EVERYTHING Included no additional fees required

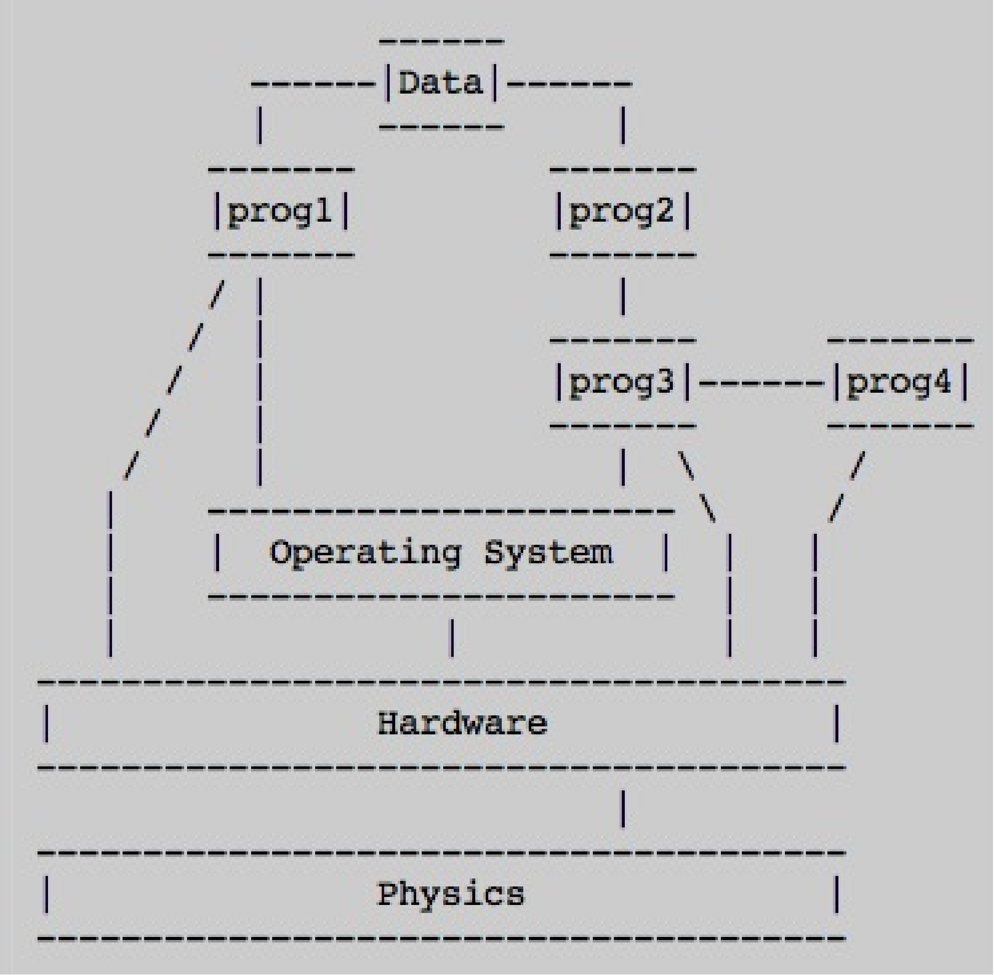
Lots of research – no funding

- My first NSA meeting
  - Circa 1986
  - A full day on site
  - Many top experts
  - Other researchers
- I show up and talk
  - My talk and questions end at 11:30 AM
  - They hand me a form to sign: national secrets
  - I refuse – the kick me out and continue...



The three best results I got

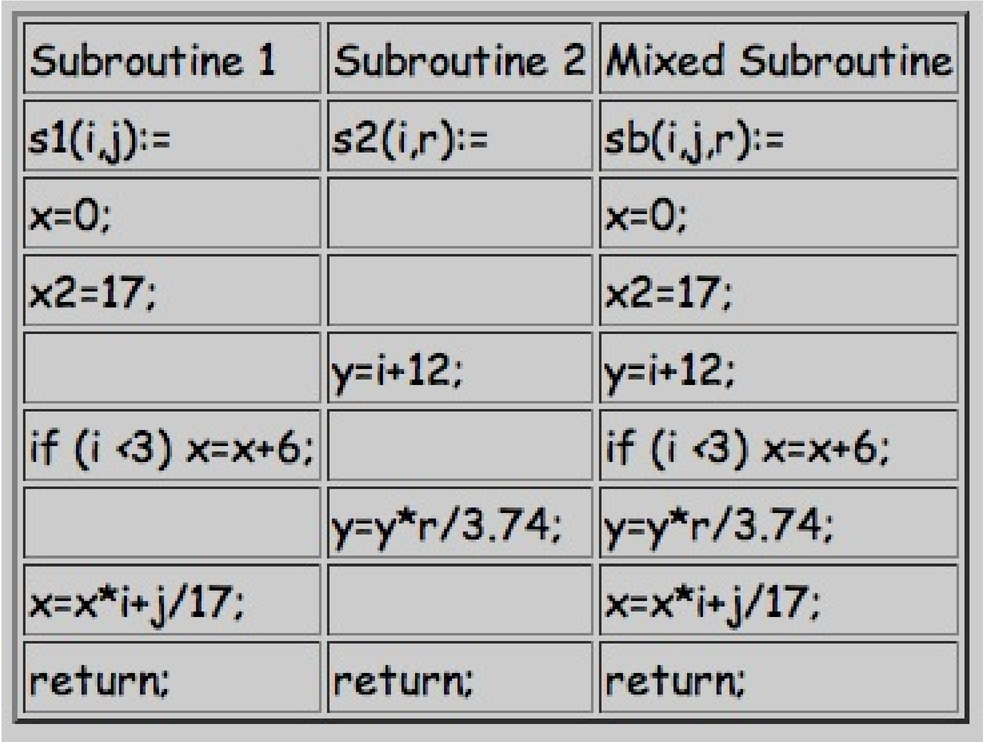
- Thanks to Matt Cohen who Trojan'ed me:
- 1988: F. Cohen, ``Models of Practical Defenses Against Computer Viruses"
- Analyze interdependencies and check supply chain of content just prior to interpretation
- “Integrity shells”: precursor of the TCG TPM
- Known virus check prior to run (Eliminator – Joe Hurst - UK)
- The integrity of content is a function of intent



```
                       ------
                ------|Data|------
                |      ------     |
             -------           -------
             |prog1|           |prog2|
             -------           -------
            /   |                 |
           /    |              -------     -------
          /     |              |prog3|------|prog4|
         /      |              -------     -------
        /       |                 |   \       /
       |    ---------------------  \     /
       |    |  Operating System |   |    |
       |    ---------------------   |    |
       |               |            |    |
   --------------------------------------------
   |                Hardware                  |
   --------------------------------------------
                          |
   --------------------------------------------
   |                Physics                   |
   --------------------------------------------
```

The three best results I got

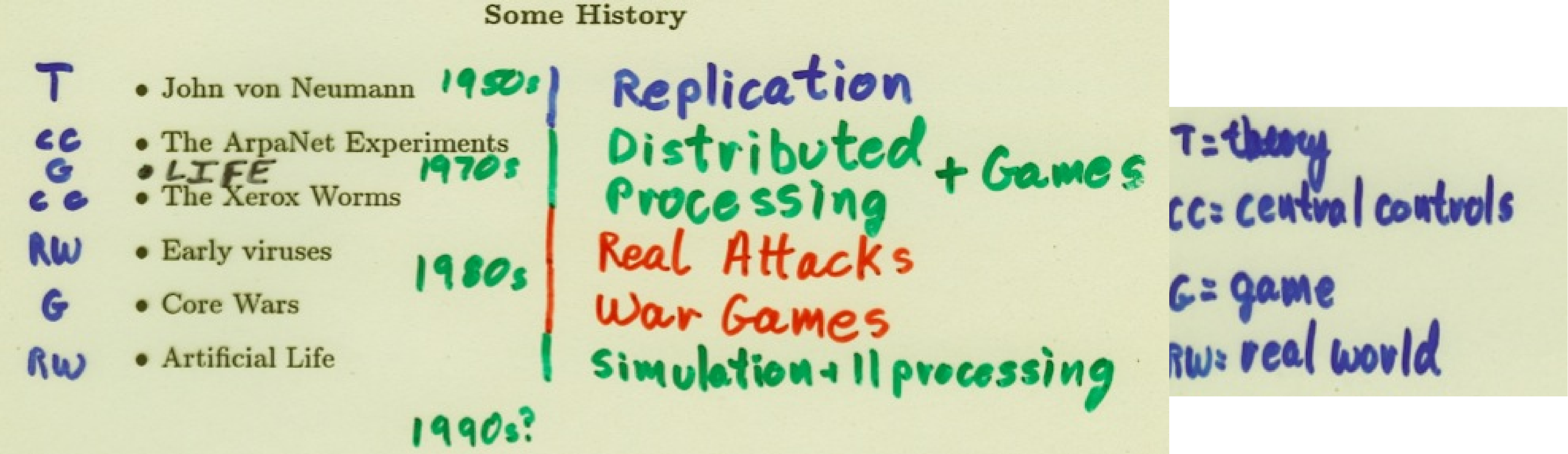
- Evolutionary defenses
  - 1992: F. Cohen, ``Operating Systems Protection Through Program Evolution"
  - Evolve the OS to give viruses a complexity problem
  - The year the IRS essentially took my house while I was in Australia



Subroutine 1	Subroutine 2	Mixed Subroutine
s1(i,j):=	s2(i,r):=	sb(i,j,r):=
x=0;		x=0;
x2=17;		x2=17;
	y=i+12;	y=i+12;
if (i <3) x=x+6;		if (i <3) x=x+6;
	y=y*r/3.74;	y=y*r/3.74;
x=x*i+j/17;		x=x*i+j/17;
return;	return;	return;

The three best results I got

- Benevolent viruses – still a controversy today?
- I did my virus work when researching for a Ph.D. In distributed computing
  - Searching for the most efficient way to distribute a computation
  - And I thought and think I found it... Reproduction!!



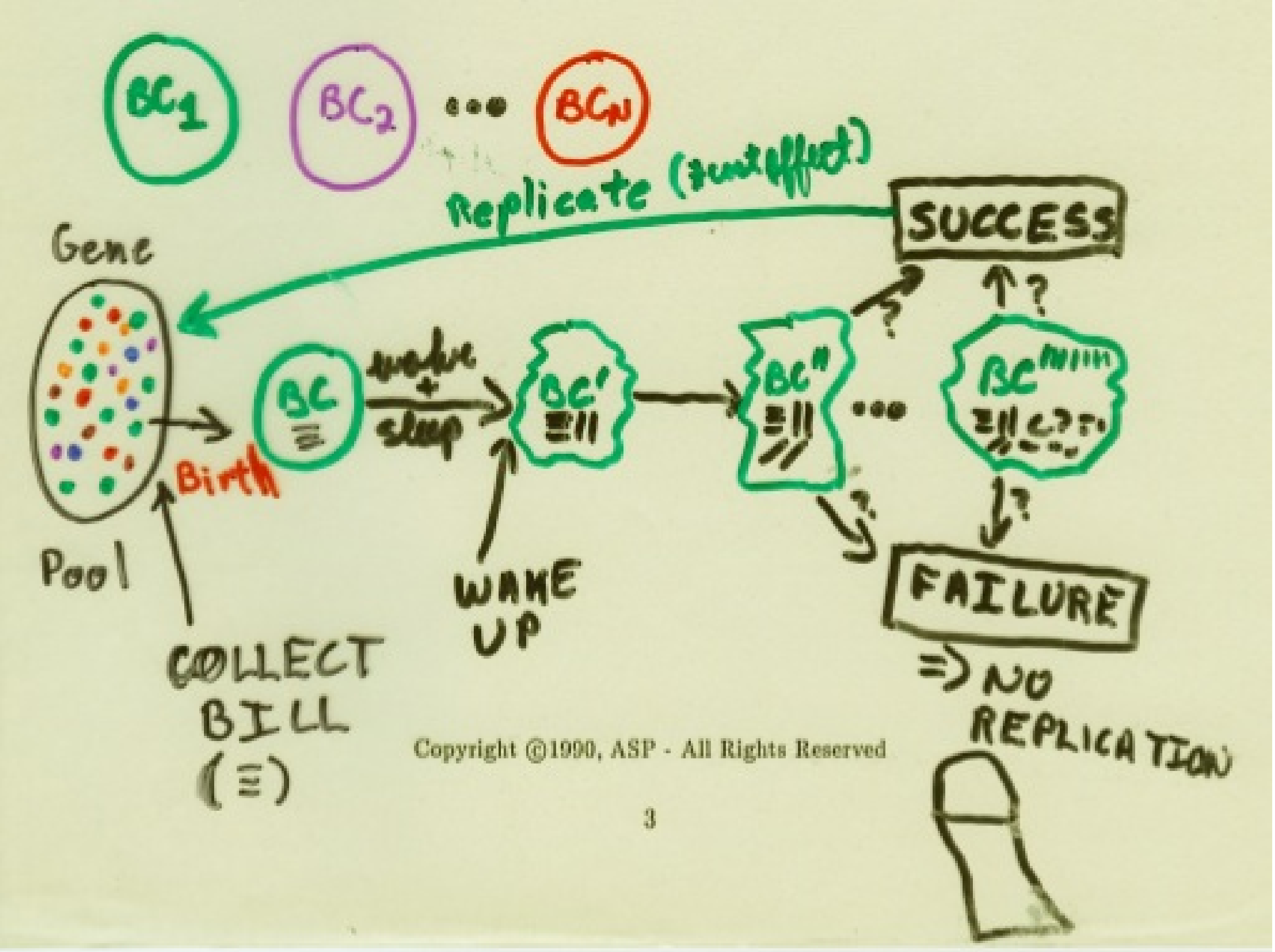
Some History

T	• John von Neumann	1950s	Replication
CC	• The ArpaNet Experiments		Distributed
G	• LIFE	1970s	Processing + Games
CC	• The Xerox Worms		
RW	• Early viruses	1980s	Real Attacks
G	• Core Wars		War Games
RW	• Artificial Life		Simulation + ‖ processing
		1990s?	

T= theory
CC= central controls
G= game
RW= real world

The viral bill collector

- A gene pool that evolves to optimize bill collection
- Prototyped
- Functioned
- LSI failed

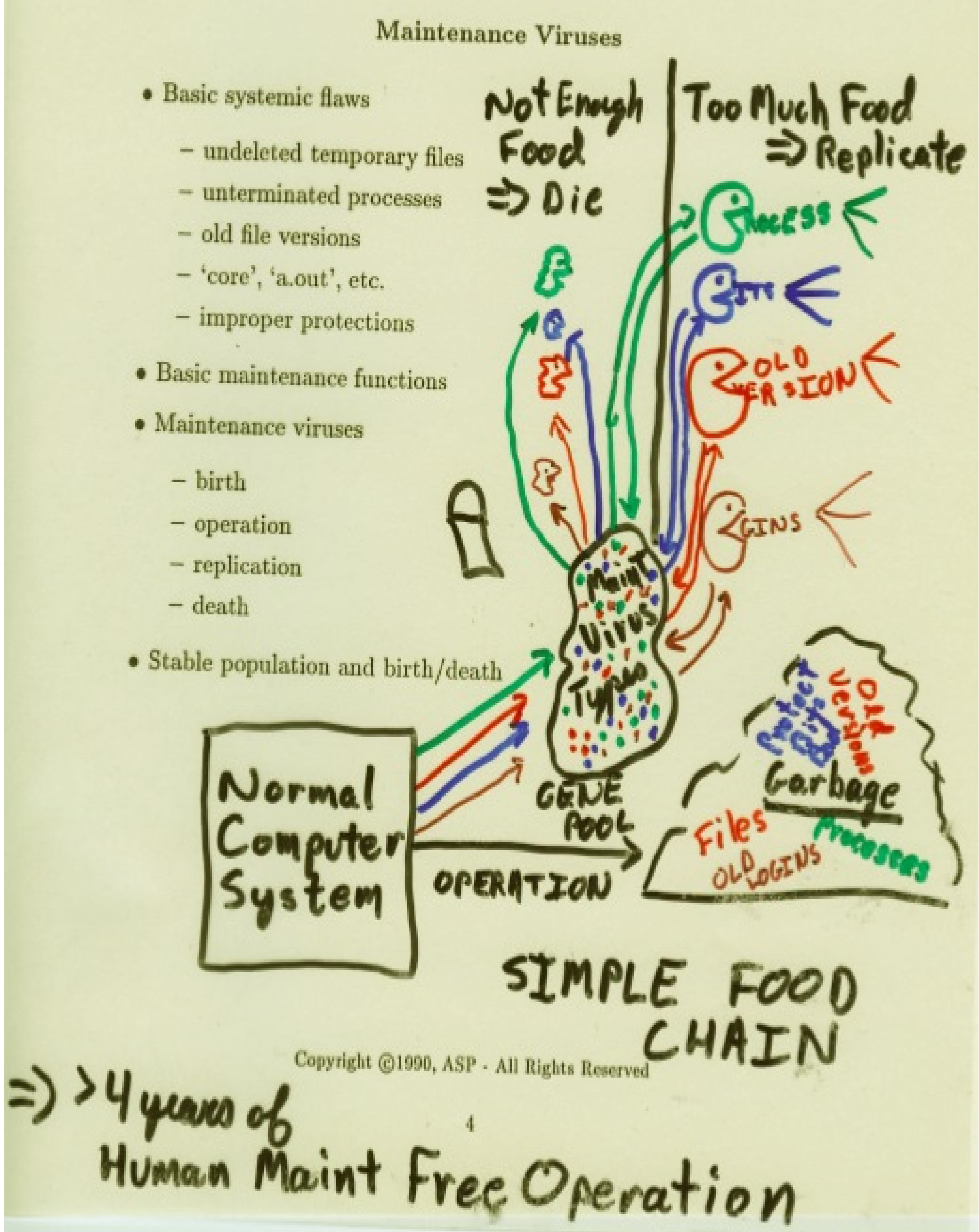


Copyright ©1990, ASP - All Rights Reserved

3

Maintenance viruses

- Implemented in Unix
- 3B2 and forward
- Maintained systems in background
- 4 years of no human intervention
- Performed all regular maintenance functions
- Operated over a small local network



Maintenance Viruses

- Basic systemic flaws
  - undeleted temporary files
  - unterminated processes
  - old file versions
  - 'core', 'a.out', etc.
  - improper protections
- Basic maintenance functions
- Maintenance viruses
  - birth
  - operation
  - replication
  - death
- Stable population and birth/death

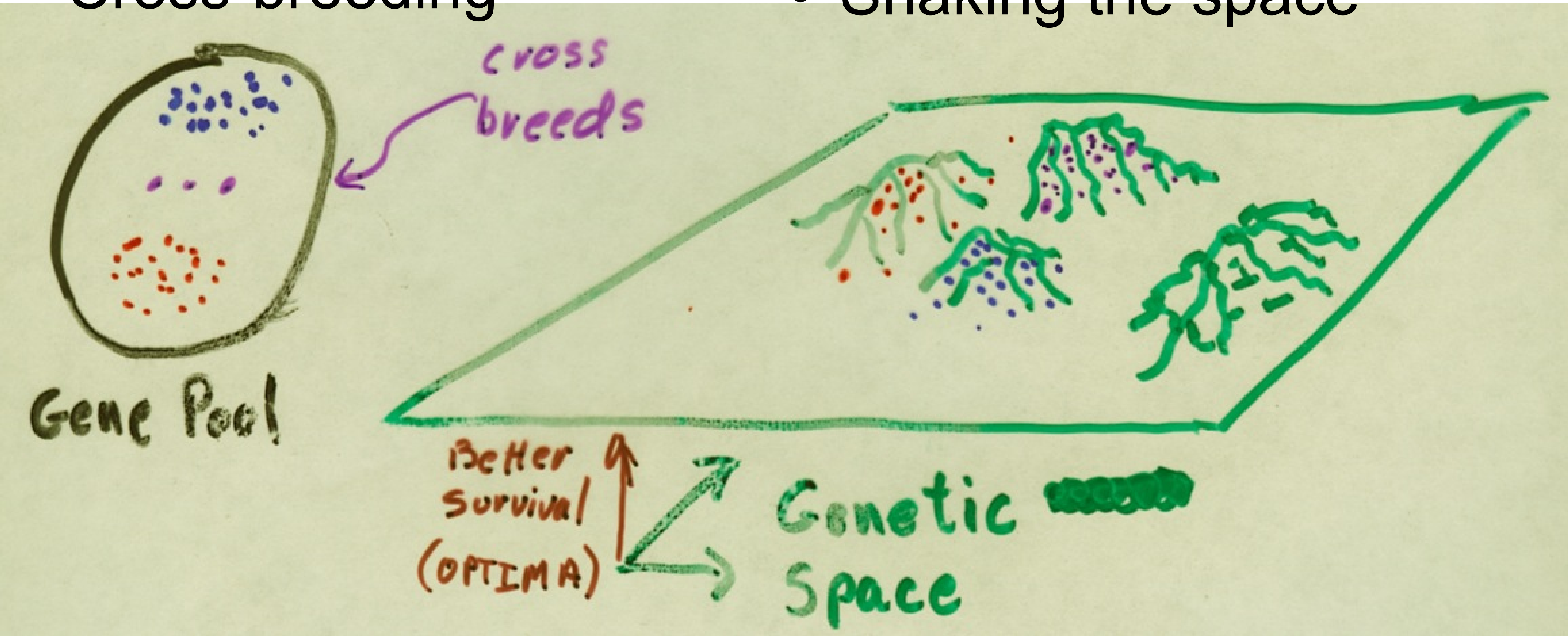
Copyright ©1990, ASP - All Rights Reserved

4

⇒ >4 years of Human Maint Free Operation

The nature of survival

- Evolution through programming
- Local optimization
- Cross-breeding
- Random variation
- Selective survival
  - F(success as task)
- Shaking the space

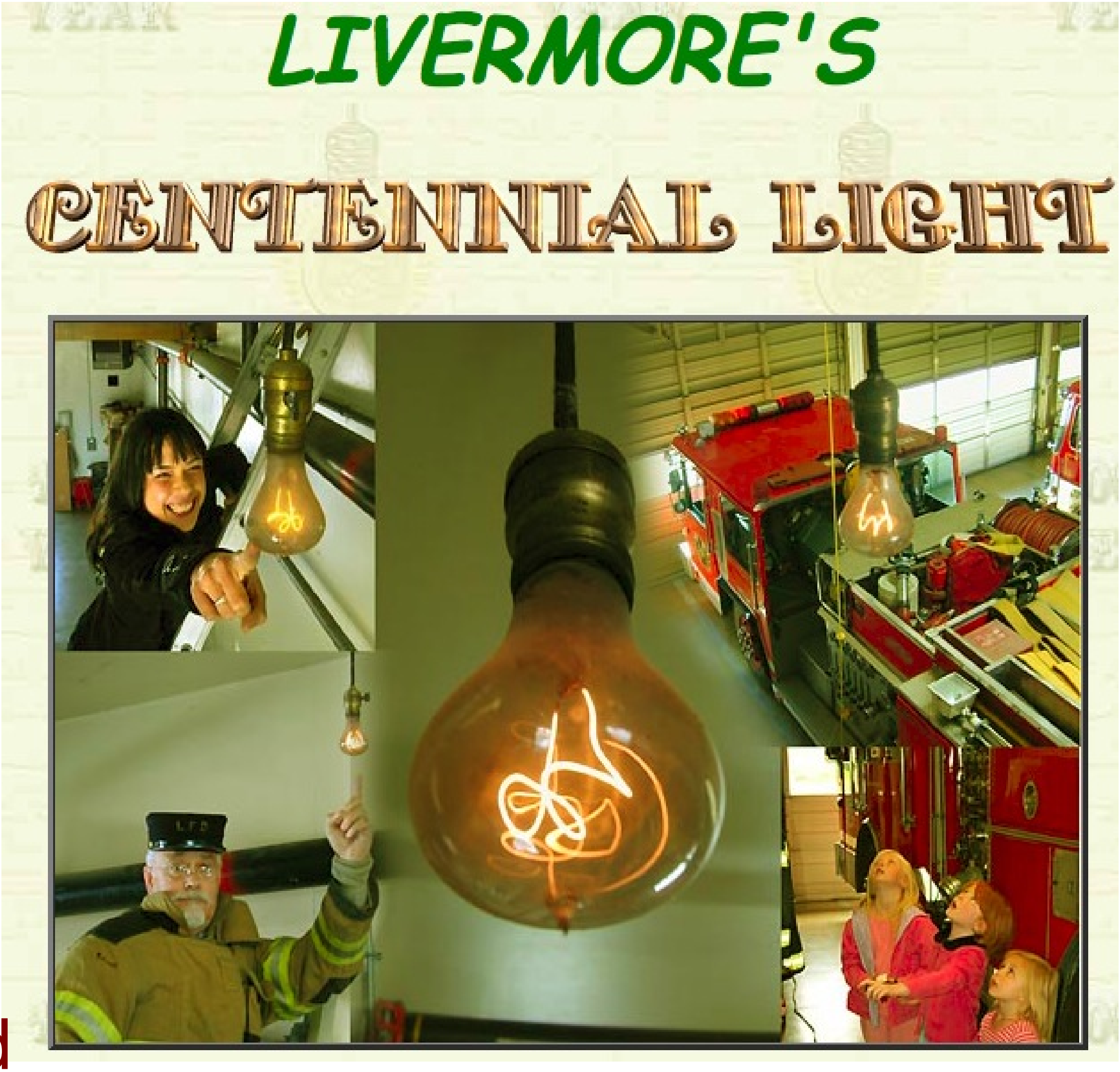


The end of AV basic research

- In 1992, I was done with it and disillusioned
  - Never $1 of research funding or other support
  - Blackballed for suggesting “benevolent viruses”
  - Auto-virus generator at 10,000/day on a PC-XT
  - Integrity toolkit was a spectacular flop (show)
  - AV companies were starting to prosper
  - I had other things to do
- A fundamental mistake I did not want to make was to stay too long in the field
- What is a business?
  - It sells again and again to the same customers

How to succeed in business

- Shelby Electric
- Made the best bulbs
- 1901: sells a bulb to the Livermore, CA fire station
- Still burning in 2009!!!
- Shelby went out of business in the 1910s
- The winners:
    - Light bulbs that must be replaced



Why hasn't AV won?

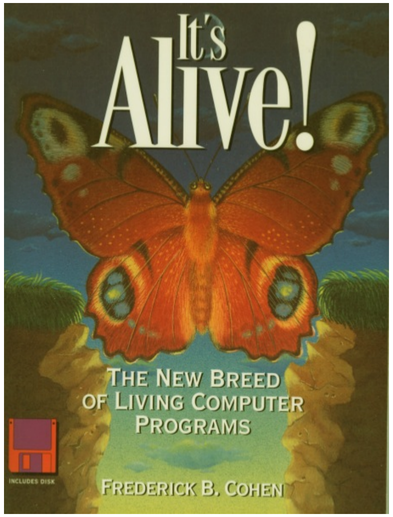
- If you win, you go out of business
- If you go out of business, you lose
- You can't win – you can only lose
- The idea is not to win – it is to survive
- How do you survive?
  - Sell things again and again to the same customers
- The customers are complicit in this
- Out of ignorance or malice, it does not matter
  - We also don't do preventive health care well

Outline

- The past...
- Simmering...
- Today
- Then what?

So I simmered

- From about 1992 till now...
  - 1992: Defensive information warfare – Information Assurance – mostly play viruses



  - 1993: Protection and Security on the Information Superhighway – mostly play viruses
  - 1994: It's Alive!!!
  - 1995: Deception for defense – mostly play viruses – and same old things repeated
  - 1998: Security simulation – some professionals and Information warfare tests
  - 2000: Large-scale distributed attack & defense
  - 2002: Digital forensics - some commercialization

Some viral search processes

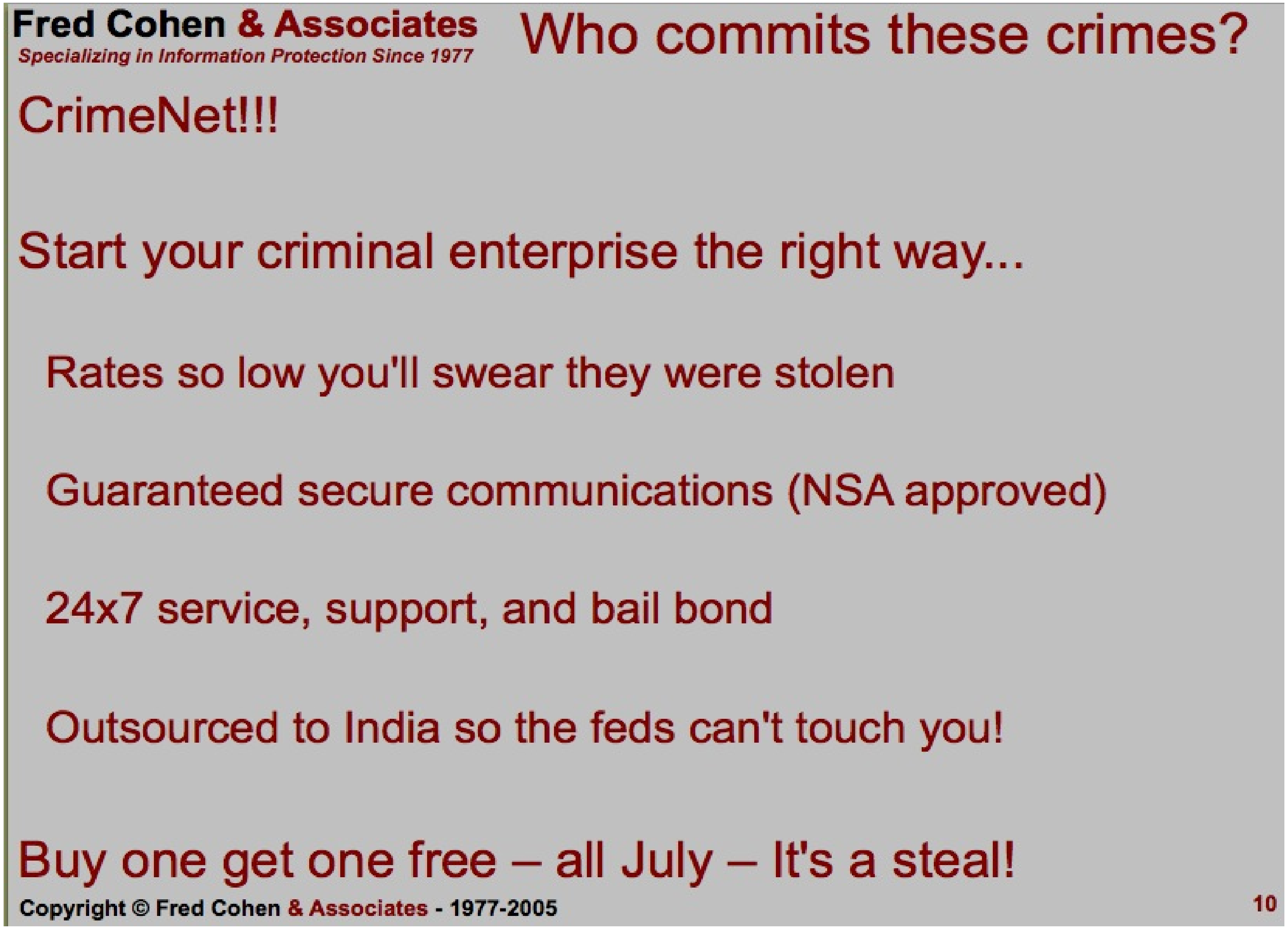
- Circa 1987:
  - Distribute a database across many computers
  - Create a search automaton for your criteria
  - Make it viral and distribute it over the database
  - As results come in, compile and present them
- 1999:
  - Viral computing used for parallel processing to do simulation of attacks and defenses
  - “Simulating Cyber Attacks, Defenses, and Consequences”

Some other viral processes

- Circa 2001 (Project Floursheim):
  - Reproduce search on many search engines
  - Download in parallel and process each result
  - Recurse on all in parallel by replicating analysis
  - Gather more results over time and do more analysis on those results
- Circa 2002 (Project resilience):
  - Distributed automated updates and a resilient infrastructure that reproduces content across and over a network and recovers spontaneously from outages

2005 - CrimeNet!!!

- My ad copy for CrimeNet circa 2005
- Then they did it!!!



Fred Cohen & Associates

Specializing in Information Protection Since 1977

Who commits these crimes?

CrimeNet!!!

Start your criminal enterprise the right way...

Rates so low you'll swear they were stolen

Guaranteed secure communications (NSA approved)

24x7 service, support, and bail bond

Outsourced to India so the feds can't touch you!

Buy one get one free – all July – It's a steal!

Copyright © Fred Cohen & Associates - 1977-2005

10

My view of science

- My view is that science should:
  - Never refuse to look at anything in detail
  - Never assume things won't change
  - Let a million flowers bloom
- My view is that in the AV arena, science failed
  - Science is failing in the security community
  - Because of closed minded attitudes
  - Because of cognitive biasses and group think
  - Because of profit over advancement
- But the times they are a changin...

Outline

- The past...
- Simmering...
- Today
- Then what?

A scientists view

- Arthur C. Clark:
  - "When a distinguished but elderly scientist states that something is possible, he is almost certainly right.
  - When he states that something is impossible, he is very probably wrong."
- I am not going to be the wrong scientist! Are you?
  - Professional virus writers have now infested more than 10% of all computers in the world and retained those infestations for periods of years despite your best efforts to stop them.
  - They use viral computing for their benefit

Viral computing today

- Whether you like it or not:
  - Google runs via viral-like computing methods
  - The largest and most successful botnets prosper by using and evolving viruses
  - Cloud computing is increasingly based on a viral model of distribution of computation
  - ~2,000 “new” (evolved) viruses/day in the wild
- Viral computing is here to stay
  - It may soon dominate the info-scape
  - How will you defend the computing clouds?
  - When they run on viral computing / distribution

Outline

- The past...
- Simmering...
- Today
- Then what?

I'm back...

- Viral computing is starting to flourish
  - How do we get it to flourish safely?
  - You cannot continue to look for “bad” in the limited way you have been – you have lost
- What can we do about it?
  - Limit sharing, function, transitivity?
    - The only theoretically feasible solutions are socially adverse to the desired utility of IT
  - Secure the platform?
    - Tried for 50 years and still fails
  - Assure integrity?
    - Integrity is a function of intent!

Then what future?

- Abandon hope all ye who enter here
  - Inscription at the gates of hell [Dante: *Devine Comedy*]
- Hope springs eternal in the human breast
  - Alexander Pope: *An Essay on Man*, 1733
- Predicting the future is easy
  - As long as you aren't worried about being right

Some alternative futures (25y)

- Viruses drop off the radar
  - People stop trying to do this and a new view/moral approach takes over (memes and IT)
  - Global IT providers decide to lock down computing for real we get predictability and reliability (IT)
  - Legal and process changes force strong attribution
  - High punishments and perpetrators are rapidly found, arrested, and put in jail for long stretches
  - Fewer authors lead to largely eliminating viruses
  - Only nation states and their sponsored groups can get away with it any more
  - Viruses used only as weapons of war – and illegal

Some alternative futures (25y)

- It just keeps going more or less like it is
  - Bad folks keep doing bad things
  - People who take advantage slowly increase their advantage until they are no longer tolerable to the populace and a form of revolution overthrows them, and round and round it goes as it has for millennia
  - Those that want to be “secure” are left out of the advantages of communication and collaboration

Some alternative futures (25y)

- Viruses take over everything
  - Viruses becomes dominant in products as providers take over all functions and content
  - Individuals become completely dependent and cowed – crooks run the world
  - Information technology goes wild and starts to evolve on its own
  - The “singularity” happens and only viruses can save humanity from the computers
    - But antivirus gets so good that humanity is wiped out by the machines... Terminator 4 – coming soon!!!

What I think most likely (25 y)

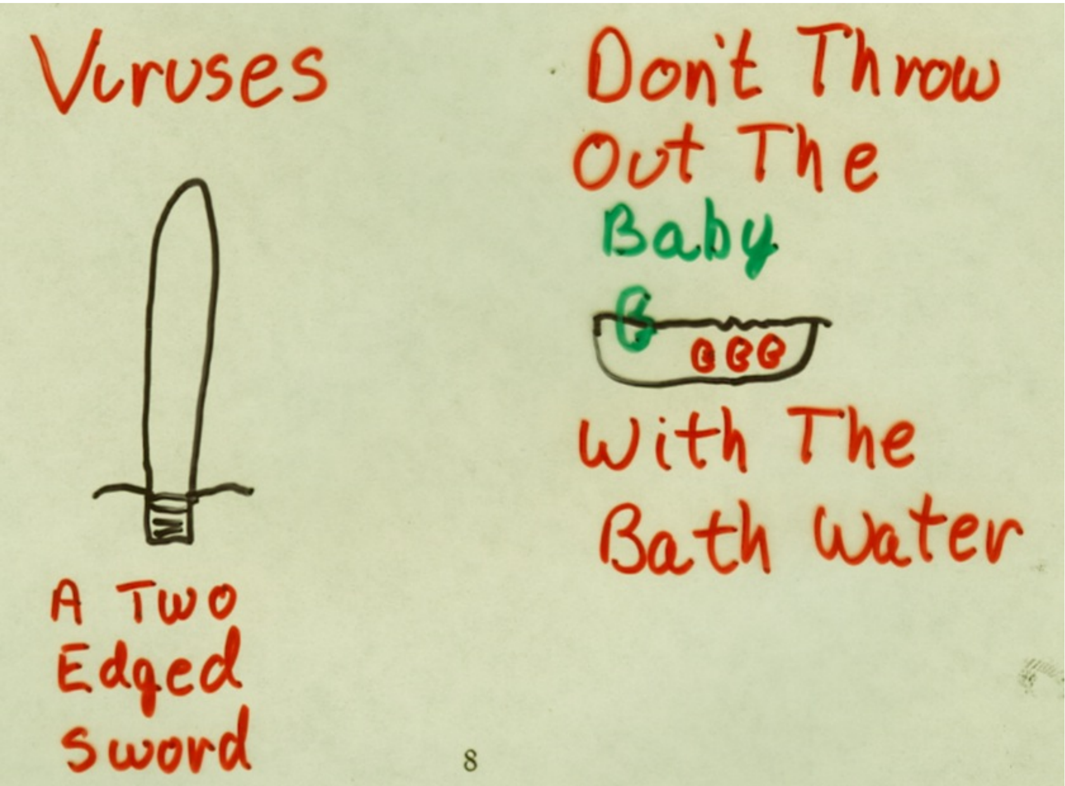
- Reduction forces:
  - Legal and process changes force strong attribution
  - AV technology becomes more “intelligent”
  - Integrity-based solutions become widespread
  - Multi-cultural IT environment reduces impact
- Momentum forces:
  - Bad folks become intolerable to societies
- Increasing forces:
  - Useful viruses become widespread and common
  - Nation-states “own” viruses as weapons of war

Defenses 25 years from now

- Attribute (recursively) all or most actions to actors
- Look for good and facilitate it – all other stays within local VM
- Integrity controls for higher-valued systems
- Monoculture yields to multi-culture
- The information age step functions continue
  - Integrity becomes a key factor in success
  - Programs emulate more human cognitive functions and make cognitive viruses key

The times they are a changin

- Viral computing is here to stay
  - Live with it!
- The threats are evolving
  - You better evolve too
- The future
  - Never as dark
  - Never as bright
  - As you imagine
- Start thinking about using viral methods to defend the infosphere / cyberspace / cloud / ...



Viruses

A Two Edged Sword

Don't Throw Out The Baby With The Bath Water

8

Thank You

http://calsci.org/ - calsci at calsci.org

http://all.net/ - fc at all.net