Computer Hacking: Viruses, Worms, and Trojan Horses

More on self-driving cars

- http://www.vox.com/2016/7/5/12077002/self-driving-cars-improve-cities
- http://www.freep.com/story/money/cars/2016/07/01/experts-worry-tesla-crash/86611662/
- http://nacto.org/wp-content/uploads/2016/06/NACTO-Policy-Automated-Vehicles-201606.pdf

- Self-driving cars need to be made fully-automated

Note

- I have placed into the web pages zip file for today the sample web pages I cite in the paper assignment
- Some other web sites that might be useful:
- http://www.chinadaily.com.cn/cndy/2010-06/09/content_9952206.htm
- http://news.xinhuanet.com/english/china/2015-05/26/c_134271001_4.htm
- http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44924&cHash=db05078399a49339345c2957196d4073#.V3rs05MrI6g

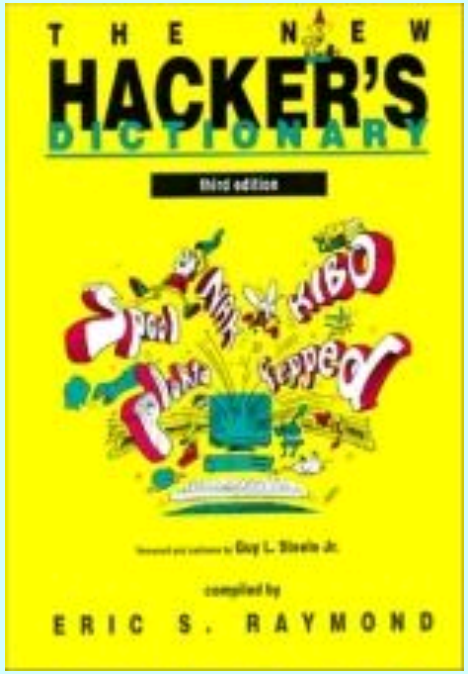
Useful news for paper 2?

- http://cra.org/govaffairs/blog/2015/01/cybersecurity-hearing-2015/
- https://science.house.gov/legislation/hearings/research-and-technology-subcommittee-and-oversight-subcommittee-hearing-cyber
- https://science.house.gov/legislation/hearings/subcommittee-energy-and-subcommittee-research-and-technology-hearing
- Testimony from several high ranking individuals – lots of interesting ideas you could explore as part of your policy paper!

Hacking on behalf of the Syrian government

- http://www.nytimes.com/2015/02/02/world/middleeast/hackers-use-old-web-lure-to-aid-assad.html
- https://www.fireeye.com/blog/threat-research/2015/02/behind_the_syrianco.html
  - Electronic conversations with Syrian opposition fighters to get them to download malware
  - "[T] he pro-Assad hackers stole large caches of critical documents revealing the Syrian opposition's strategy, tactical battle plans, supply requirements and data about the forces themselves"

What is hacking?



In the days when Sussman was a novice, Minsky once came to him as he sat hacking at the PDP-6.

"What are you doing?", asked Minsky.

"I am training a randomly wired neural net to play Tic-tac-toe", Sussman replied.

"Why is the net wired randomly?", asked Minsky.

"I do not want it to have any preconceptions of how to play", Sussman said.

Minsky then shut his eyes. "Why do you close your eyes?" Sussman asked his teacher.

"So that the room will be empty."

At that moment, Sussman was enlightened.

Definitions

- A person who enjoys learning the details of computer systems and how to stretch their capabilities
- A person who programs enthusiastically
- A person capable of appreciating hack value
- A person good at programming quickly
- An expert on a particular program

Definitions, continued

- An expert of any kind
- A creative practical joke
- An malicious meddler who tries to find information by poking around

Timeline of Early Incidents

1971 "Captain Crunch" attacks the phone system.

1982 John Shoch and Jon Hupp of Xerox PARC publish a paper on how worm programs allow for distributed computing.

1983 In the movie *WarGames,* Matthew Broderick's character gains access to the military's nuclear command system.

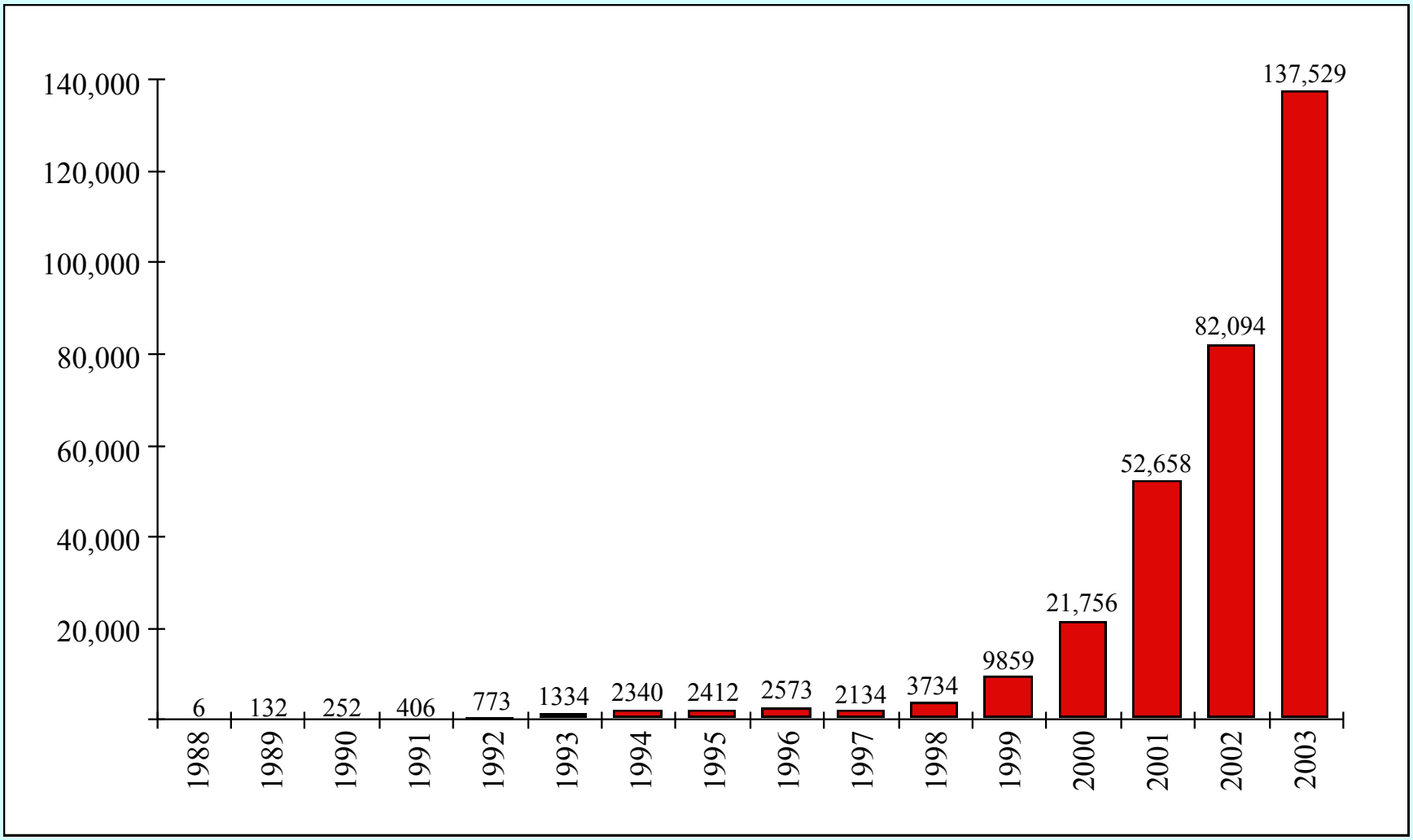
1984 A group of Milwaukee teenagers—known as the 414's after the area code—begins a series of break-ins.

1986 Cliff Stoll begins stalking the "Wily Hacker."
1986 First major PC virus released (*Brain* or *Pakistani* virus)
1987 "Captain Midnight" - first high-tech terrorism

1988 Robert Morris releases the Internet Worm.

1990 Secret Service conducts "Operation Sundevil" raids.

CERT Incident Report



Principal Modes of Software Attack

1. Viruses
2. Worms
3. Trojan horses
4. Security loopholes
5. Denial-of-service attacks
6. Logic bombs
7. Spyware/Adware

"Social engineering"

Viruses

- A computer virus is a program that inserts itself into one or more files and then performs some (possible null) action

From Matt Bishop's Computer Security

The Internet Worm, 1988

"All the News That's Fit to Print"

The New York Times

Late Edition
New York: Today, partly sunny, milder. High 59-64. Tonight, mostly cloudy. Low 48-54. Tomorrow, cloudy, windy, rain developing. High 57-62. Yesterday: High 58, low 41. Details, page D16.

VOL. CXXXVIII... No. 47,679 NEW YORK, FRIDAY, NOVEMBER 4, 1988 35 CENTS

Gov. Michael S. Dukakis having his picture taken by a 10-year-old fan at a town meeting in Fairless Hills, Pa., during a tour of the Northeast in which he emphasized the drug problem. Page A19. Vice President Bush addressed supporters a rally in Columbus, Ohio. Less than a week after Mr. Dukakis acknowledged being a liberal, Mr. Bush said yesterday that "this election is not about labels." Page A18.

'Virus' in Military Computers Disrupts Systems Nationwide

By JOHN MARKOFF

[illegible] questions about the vulnerability of the nation's computers, a Department of Defense network has been disrupted since Wednesday by a rapidly spreading "virus" program apparently introduced by a computer science student.

The program reproduced itself through the computer network, making hundreds of copies in each machine it reached, effectively clogging systems linking thousands of military, corporate and university computers around the nation and preventing them from doing additional work. The virus is thought not to have destroyed any files.

By late yesterday afternoon computer experts were calling the virus the largest assault ever on the nation's computers.

'The Big Issue'

"The big issue is that a relatively benign software program can virtually bring our computing community to its knees and keep it there for some time," said Chuck Cole, deputy computer security manager at Lawrence Livermore Laboratory in Livermore, Calif., one of the sites affected by the intrusion. "The cost is going to be staggering."

Clifford Stoll, a computer security expert at Harvard University, added: "There is not one system manager who is not tearing his hair out. It's causing enormous headaches."

The affected computers carry a tremendous variety of business and research information among military officials, [illegible] and corporations.

While some sensitive military data are involved, the computers handling the nation's most sensitive secret information, like that on the control of nuclear weapons, are thought not to have been touched by the virus.

Parallel to Biological Virus

Computer viruses are so named because they parallel in the computer world the behavior of biological viruses. A virus is a program, or a set of instructions to a computer, that is either planted on a floppy disk meant to be used with the computer or introduced when the computer is communicating over telephone lines or data networks with other computers.

The programs can copy themselves into the computer's master software, or operating system, usually without calling any attention to themselves. From there, the programs can be passed to additional computers.

Depending upon the intent of the software's creator, the program might cause a provocative but otherwise harmless message to appear on the computer's screen. Or it could systematically destroy data in the computer's memory. In this case, the virus program did nothing more than reproduce itself rapidly.

The program was apparently a result of an experiment, which

Continued on Page A21, Column 2

Registration Off Since 1984 Vote

There has been a pronounced decline in the percentage of eligible Americans who are registered to vote, a research group reports.

Nationally, the percentage of eligible Americans who are registered is estimated to be 78.3 percent, down 2.2 points from the 1984 level.

The group's study concluded that in many of the 30 states where final figures are available the decline was among

PENTAGON REPORTS IMPROPER CHARGES FOR CONSULTANTS

CONTRACTORS CRITICIZED

Inquiry Shows Routine Billing of Government by Industry on Fees, Some Dubious

By JOHN H. CUSHMAN Jr.
Special to The New York Times

WASHINGTON, Nov. 3 — A Pentagon investigation has found that the nation's largest military contractors routinely charge the Defense Department for hundreds of millions of dollars paid to consultants, often without justification.

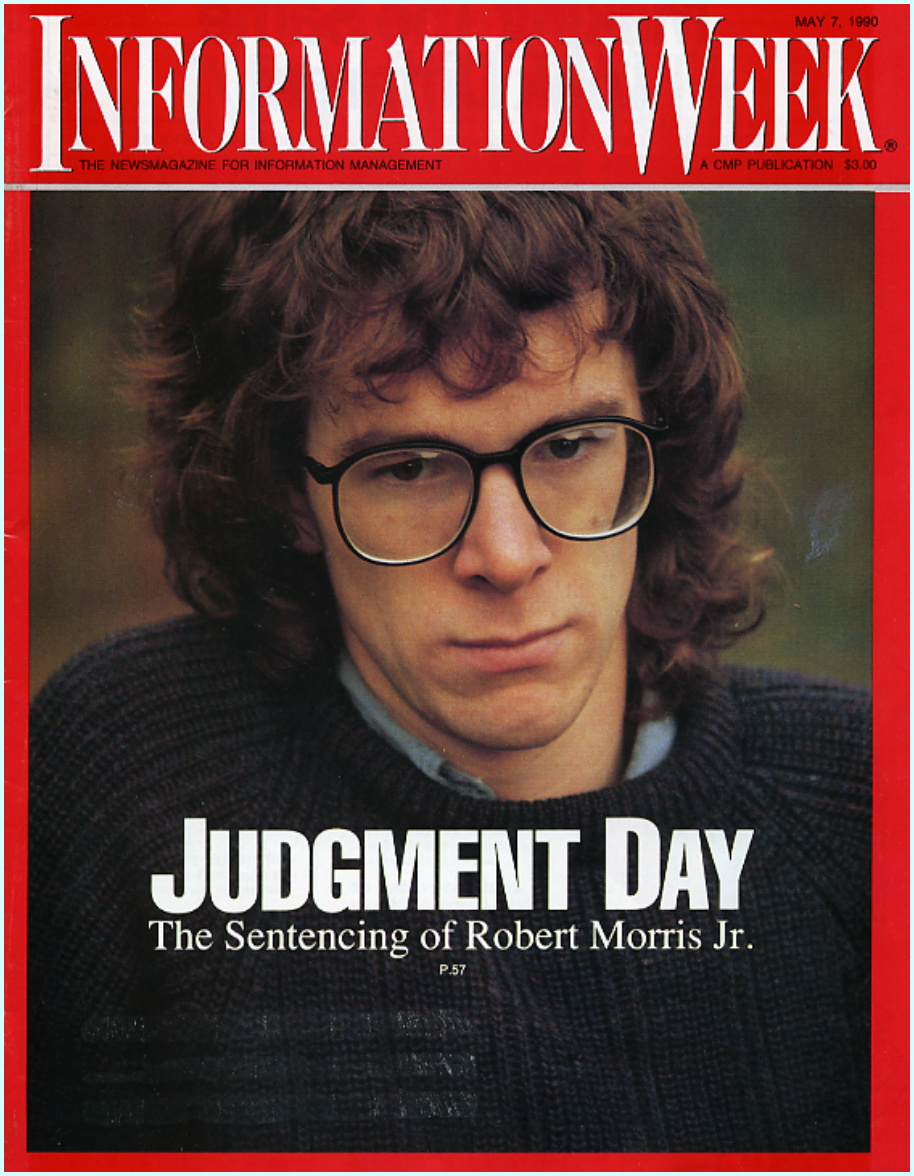
The report of the investigation said that neither the military's current rules nor the contractors' own policies are adequate to assure that the Government does not improperly pay for privately arranged consulting work. Senior Defense Department officials said the Pentagon was proposing changes to correct the flaws.

While it is not improper for military contractors to use consultants in performing work for the Pentagon, the work must directly benefit the military if it is to be paid for by the Defense Department. Often, Pentagon investigators discovered, this test is not met.

Broader Look at Consultants

The Justice Department's continuing criminal investigation has focused attention on consultants and their role in the designing and selling of weapons, and the Defense Department has been criticized for using consultants too freely. Now the Pentagon's own inves-

Robert Morris Jr.



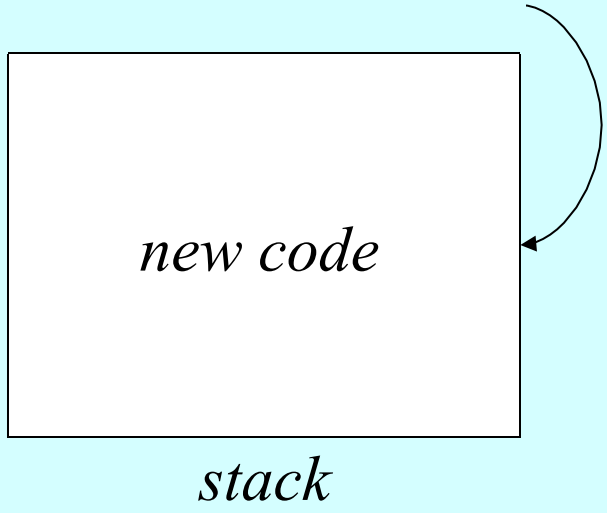
Strategies Employed by the Internet Worm

- The **`debug`** option in Unix **`sendmail`**
- The **`fingerd`** attack
- Password guessing
- Use of **`rhosts`** files

The FingerD Attack

If the user, however, enters a name string that overflows the buffer, the bytes in that name will overwrite the data on the stack.

Now when the function returns, it will jump into the code written as part of the name, thereby executing the worm's instructions.



Trojan Horses

Ken Thompson on Trojan Horses

Ken Thompson, one of the developers of Unix, discussed the problem of computer security—and Trojan Horses in particular—in his Turing Award lecture of 1983. His talk illustrated the Trojan Horse concept is in the optional reading.

The key point to take from Ken's example is that it is possible to build a Trojan Horse—what *WarGames* calls a "back door"—and then completely cover all traces of that back door in the source code.

Ken Thompson. 1984 "Reflections on Trusting Trust." CACM 27(8) 761-763 (August)

Security loopholes

- A vulnerability in a system that allows an attacker to attack/compromise a system

Denial of Service Attacks

- E.g. rabbits and bacteria
- Malicious logic that multiplies very quickly leading to system resources becoming exhausted

Logic bombs

- A program that violates a security policy when an external event occurs

Spyware/Adware

- Installed as part of another program – reports back what the victim is doing

Social Engineering

- Popularized by Kevin Mitnick
- Several techniques, including:
  - Pretexting
  - Phishing

Is hacking good?

- Can lead to awareness of a system's vulnerabilities and allowing for defenses to be prepared
- Can lead to availability of information - e.g. social protection
- The GNU Manifesto

Is hacking bad?

- You can explain a system vulnerability without breaking into it.
- Privacy loss
- Complete government transparency isn't always good
- Social protection leads agencies to increased secrecy

Ideas from Spafford, 1992. “Are Computer Hacker Break-ins Ethical?” Journal of Systems Software 17:41-47