The Internet Worm + 10 Years:
Lessons Learned and Not Learned
Eugene H. Spafford
Purdue University CERIAS

Today in History
- Peter the Great crowned as Tsar in Russia, 1721
- Daniel Boone born in 1734
- James Polk (11th U.S. President) born in 1795
- Warren Harding (29th U.S. President) born in 1865
- Actor Burt Lancaster born in 1913
- Actor Ray Walston born in 1914
- Truman defeats Dewey in Presidential election, 1948
- Robert T. Morris sets loose the Internet Worm in 1988
The Internet in 1988

- The global set of computers connected together using IP protocols.
- Included:
  - Arpanet
  - Milnet
  - NSFnet
  - CSnet
- About 60,000 interconnected systems in October 1988. 85% used UNIX or one of its variants.

The Worm

- Written as an “experiment” by graduate student Robert T. Morris.
- It affected only Vax and Sun computers running UNIX or its variants.
- Altered no files, disclosed no information, changed nothing on the system – just replicated out of control.
- First infection appeared to be on prep.ai.mit.edu
**The Worm: What it Did**

- The worm replicated by means of a small bootstrap program that copied over binary versions of the worm, plus auxiliary files.
- The bootstrap was introduced via one of three methods:
  - debug option in sendmail
  - buffer overrun in finger daemon
  - taking advantage of trusted hosts in rlogin and rsh commands

**Chronology**

- Worm developed over a period of weeks in October 1988 @ Cornell. Some code may have been developed earlier.
- Dispatched on a machine at MIT around 8pm on 2 November 1988.
- Dozens of machines compromised by midnight. As many as 4000 infected by noon of the next day.
Eradication

- Spotted within hours of its release.
- Effective preventative measures identified within 12 hours.
- Definitive preventative identified and publicized within 24 hours.
- Decompiled version available within 36 hours.
- Internet almost completely back to normal within 72 hours.
  - *despite these efforts, some Worm activity was seen for more than 30 days!*

Immediate Aftermath

- Some sites did not rejoin the network.
- Crisis centers were established, including the CERT/cc.
  - Robert T. Morris was convicted of a US Federal felony. He was given a probated sentence.
  - Many new instances of worms and viruses, probably as a direct result of the publicity.
  - Many new (mostly poor) laws were proposed.
  - Little new understanding or study of worms done.
  - Forensic tools were not developed
Growth of the Problem

Reported new incidents of IBM-PC viruses and wide-scale network worms.

Things We Learned

- We lacked good analysis tools
- Too much homogeneity
- We needed secondary methods of communication
  - We needed a central “clearinghouse”
  - We needed better audit facilities
- The press needed to be better educated about these kinds of threats
- Needed to protect mailers better
- Poor trust relationships leads to danger
- Poor programming poses problems
We lack good analysis tools

- In 1988 we didn’t have any good tools to go from binary code to source code so as to analyze attack software.
- In 1998 we still don’t have any such tools. Furthermore, the WIPO legislation of 1998 now makes creation of such tools against the law!

Too much homogeneity

- In 1988, 85% of the Internet was Unix. Luckily, there were about 20 different variants in use.
- In 1998, there are fewer versions of Unix in place. In most enterprise and office LANS, Windows variants approach 100%. Both macro and micro environments are too homogeneous.
We needed secondary methods of communication

- In 1988 we didn’t have alternate means of communication among major network players when the Internet ‘went down.’
- In 1998 things are little better. In fact, with the worldwide scope, it is not clear that any existing mechanism will reach all parties quickly.

We needed a central “clearinghouse”

- In 1988 we had no central place to contact when an emergency arose
- In 1998 we have the CERT/cc, the NIPC, the vendors, bugtraq, the CIAC, the FIRST, and several dozen hacker groups. Who’s in charge?
We needed better audit facilities

- In 1988 we used ad-hoc auditing derived from old accounting mechanisms to determine what happened on the system.
- In 1998 we use ad-hoc auditing derived from network sniffers and old accounting mechanisms.

The press needed to be better educated

- In 1988 the press didn’t know a worm from a virus from a bug.
- IN 1998 things have improved with some press, but the readership doesn’t grasp the difference.
Needed to protect mailers better

In 1988, sendmail was found to contain flaws that compromised systems.

In 1998, sendmail was found to contain flaws that compromised systems. So was Eudora, Netscape Communicator, and Microsoft Outlook.

Poor trust relationships leads to danger

Users without clear understanding of security concerns exposed the enterprise to danger via the rsh/rhosts mechanism.

Users without clear understanding of security concerns expose the enterprise to danger via the WWW and MIME.
Poor programming poses problems

- In 1988, a series of buffer overflow problems led to trusted programs being compromised
- In 1998, there has been a long series of buffer overflow problems in trusted programs.

Conclusions?

We have done a terrible job of learning from the past and integrating the lessons learned into the practice of security.

The Internet is not necessarily safer today than in 1988.

With the advent of ActiveX, macro viruses, and user-downloaded applications, a cousin of the Worm is feasible.

We need to do something to learn from the past and build a proper security infrastructure!
The Weight of Events

- Over $10 billion in on-line commerce this year will attract miscreants
- Network population and access continuing to surge
- On-line
  - Over 200 million users
  - In over 150 countries
  - Increasing at a rate of 150% per year
    All with access to your networks?

Limited personnel

- Trained infosec professionals for the current environment are in short supply.
- Protection requires far more training than does attacking
- Few venues for appropriate training and education exist
- The wrong types are being hired because of the shortage of properly-trained personnel.
The View from Academia

Consider that there are only two major dedicated academic infosec centers in the country (and fewer than 6 overall). Total PhD production from these places is about 3 a year. We are in a crisis, and there is no on-going government support for the research & education missions.

COAST & CERIAS

COAST Laboratory founded in 1992.
- Almost 100 students involved in projects since then
- 10 involved faculty
- A dozen sponsoring companies and agencies
- Significant output of technology, papers, personnel in CS
- World-leading reputation

CERIAS founded in 1998.
- Taking a broader view of the infosec problem:
  CERIAS is multidisciplinary in nature and will address the problems of information protection from a variety of different perspectives.
- Faculty involved from across the university
- Over 60 students and 20 faculty
- Subsumes COAST
Disciplines Currently Represented

- Computer Sciences
- Education
- Electrical and Computer Engineering
- English
- Industrial Engineering
- Linguistics
- Management
- Philosophy
- Political Sciences

More to Come …

Current Sponsors

- Sponsors
  - AT&T GeoPlex
  - Cisco Systems
  - DoD–NSA
  - Global Integrity Corp.
  - Microsoft
  - MITRE
  - Schlumberger
  - Sprint
  - Sun Microsystems

- Other Donors & Supporters
  - Internet Security Systems
  - Addison-Wesley
  - O’Reilly & Associates
  - Tektronix

...and new sponsor, Hewlett-Packard!
Yeah, but suppose the metaphor ran in the OTHER direction. Suppose the HIGHWAYS were like the NET. All right! Severe craziness. A highway HUNDREDS of lanes wide. Most with potholes. Privately operated bridges and overpasses. No highway patrol. A couple of rent-a-cops on bicycles with broken whistles. 500 member VI GILANTE POSSES with nuclear weapons. 237 ON RAMPS at every intersection. NO SIGNS. Wanna get to Ensenada? Holler out the window at a passing truck to ask directions. AD HOC traffic laws. Some lanes would VOTE to make use by a single-occupant-vehicle a CAPITAL OFFENSE on Monday through Friday between 7:00 and 9:00. Other lanes would just SHOOT you without a trial for talking on a car phone.

AOL would be a giant diesel-smoking BUS with hundreds of EBOLA victims and a TOILET spewing out on the road behind it. Throwing DEAD WOMBATS and rotten cabbage at the other cars most of which have been ASSEMBLED AT HOME from kits. Some are 2.5 horsepower LAWNMOWER ENGINES with a top speed of nine miles an hour. Others burn NITROGLYCERINE and IDLE at 120. No license tags. World War II BOMBER NOSE ART instead. Terrifying paintings of huge teeth or VAMPIRE EAGLES. Bumper mounted MACHINE GUNS. Flip somebody the finger on this highway and get a WHITE PHOSPHORUS GRENADE up your tailpipe. Flatbed trucks with ANTI-AIRCRAFT MISSLE BATTERIES to shoot down the KRUD Traffic Watch helicopter. A little kid on a tricycle with a squirrjgun filled with HYDROCHLORIC ACID.

NO OFFRAMPS.

Now THAT’S the way to run an Interstate Highway system.
Thank You!