Open source security lessons

Wietse Venema

IBM T.J. Watson Research

Hawthorne, NY, USA

Dawn of the Internet age in Eindhoven, The Netherlands

- Eindhoven university was among the first universities in the Netherlands to get an Internet connection.
- This attracted a number of users who had no official relationship with the university.
- Most unofficial users were careful not to draw attention to their activities.
- Unfortunately, there was one exception...

Lesson one: TCP Wrapper

rm -rf / &

Lesson one: TCP Wrapper

Challenges

- Problem: empty disks don’t reveal how intrusions happen.
- Solution: instrument the network software to log activity *before* the disaster happens.
- Problem: no source code for the network software from SUN, Digital, Apollo, HP, IBM, etc. No expertise and no authority to change those systems anyway.
- Solution: the smallest possible program to log the type and origin of network connections.

```
main(argc, argv)
int     argc;
char  **argv;
{
    openlog(argv[0], LOG_PID, LOG_MAIL);
    if (getpeername(0, &sa, &length) < 0) {
        syslog(LOG_ERR, "getpeername: %m");
        host_name = "unknown";
    } else if (hp = gethostbyaddr(&sa.sin_addr,
                      sizeof(sa.sin_addr), AF_INET)) {
        host_name = hp->h_name;
    } else {
        host_name = inet_ntoa(sin.sin_addr);
    }
    syslog(LOG_INFO, "connect from %s", host_name);  /* XXX */
    execv(REAL_DAEMON, argv);
    syslog(LOG_ERR, "%s: %m", REAL_DAEMON);
}
```

```
date   time     hostname service  content of logged message
May 21 14:06:53 tuegate: systatd: connect from monk.rutgers.edu
May 21 16:08:45 tuegate: systatd: connect from monk.rutgers.edu
May 21 16:13:58 trf:     systatd: connect from monk.rutgers.edu
May 21 18:38:17 tuegate: systatd: connect from ap1.eeb.ele.tue.nl

May 21 23:41:12 tuegate: systatd: connect from mcl2.utcs.utoronto.ca
May 21 23:48:14 tuegate: systatd: connect from monk.rutgers.edu
May 22 01:08:28 tuegate: systatd: connect from HAWAII-EMH1.PACOM.MIL
May 22 01:14:46 tuewsd:  fingerd: connect from HAWAII-EMH1.PACOM.MIL
May 22 01:15:32 tuewso:  fingerd: connect from HAWAII-EMH1.PACOM.MIL
May 22 01:55:46 tuegate: systatd: connect from monk.rutgers.edu
May 22 01:58:33 tuegate: systatd: connect from monk.rutgers.edu
May 22 02:00:14 tuewsd:  fingerd: connect from monk.rutgers.edu
May 22 02:14:51 tuegate: systatd: connect from RICHARKF-TCACCIS.ARMY.MIL
May 22 02:19:45 tuewsd:  fingerd: connect from RICHARKF-TCACCIS.ARMY.MIL
May 22 02:20:24 tuewso:  fingerd: connect from RICHARKF-TCACCIS.ARMY.MIL

May 22 14:43:29 tuegate: systatd: connect from monk.rutgers.edu
May 22 15:08:30 tuegate: systatd: connect from monk.rutgers.edu
May 22 15:09:19 tuewse:  fingerd: connect from monk.rutgers.edu
May 22 15:14:27 tuegate: telnetd: connect from cumbic.bmb.columbia.edu
May 22 15:23:06 tuegate: systatd: connect from cumbic.bmb.columbia.edu
May 22 15:23:56 tuewse:  fingerd: connect from cumbic.bmb.columbia.edu
```

COMPUTER INTRUDERS TAPPING U.S. SYSTEMS

By JOHN MARKOFF

Beyond the reach of American law, a group of Dutch computer intruders have been openly defying United States military, space and intelligence authorities for almost six months.

- - -

U.S. government officials said that they had been tracking the interlopers, but that no arrests had been made because there are **no legal restrictions in the Netherlands** barring unauthorized computer access.

New York times, April 21, 1991.

Wrapping up this episode

- The intruder operated as **rchack** in Eindhoven, **adrian** in Stanford, and as **berferd** in Bell Labs.
- Having found out that he was being watched, our suspect stopped and was never arrested.
- Two years later, computer hacking became illegal in the Netherlands.
- Wietse's TCP Wrapper has been installed on millions of systems.
- Lesson: when resources are limited, become creative.

April 5, 1995 - Death of the Internet Predicted

“It’s like randomly mailing automatic rifles to 5,000 addresses. I hope some crazy teen doesn’t get a hold of one.”

Oakland Tribune

“It’s like distributing high-powered rocket launchers throughout the world, free of charge, available at your local library or school.”

San Jose Mercury

White paper: Improving the security of your site by breaking into it

- Co-authored with Dan Farmer (COPS, Coroner's toolkit).
- Explained the risks of
  - "out of the box" insecure system configurations,
  - inherently dangerous network services,
  - not installing bug fixes for known vulnerabilities.
- Made recommendations for secure operation.
- Announced network security checking tool SATAN[1] that would *automatically* identify vulnerable systems.

[1]Security Administrator Tool for Analyzing Networks

Restricted release versus controlled release

Restricted release:

- Don’t release this program - it’s the end of civilization.
- Give it to the good guys only (10,000 organizations).
- Give it to the rich guys only (rich guys are good guys).

Controlled release:

- Give alpha test copies to vendors, CERTs, other experts.
- Give early demo version to the public.
- Give final version to everyone (balance of arms).

The day after - post-release aftermath

- Featured on CNN.
- San Francisco Chronicle headline:

  HELL DIDN'T BREAK LOOSE WITH SATAN

- And other "Man Didn't Bite Dog" stories.
- Slash-dot effect years before slash-dot was created.
- No significant *increase* in break-in activity (according to query by Eugene Spafford among CERT teams).
- No significant *decrease* in break-in activity, either :-(

SATAN episode impact

- This was just another episode in the ongoing debate about disclosure of (software) vulnerabilities.
- As one US military person put it, “if my computer systems have a problem, then I’d rather hear it from a friend than from an enemy”.
- Meanwhile, network security scanning has become standard practice, just like intrusion detection, virus detection, and so on.
- Lesson: free publicity is worth every penny you pay for it.

SHARING SOFTWARE, IBM TO RELEASE MAIL PROGRAM BLUEPRINT

By JOHN MARKOFF

- - -

The program, **Secure Mailer**, serves as an electronic post office for server computers connected to the Internet. It was developed by **Wietse Venema**, an IBM researcher and computer security specialist.

- - -

Currently about 70 percent of all e-mail worldwide is handled by **Sendmail**, a program that has been developed over more. . .

New York times, December 14, 1998.

CERT/CC advisories for Sendmail, once majority carrier of Internet email

Advisory	Version	Impact
CA-1988-01	5.58	Unprivileged access
CA-1993-16	8.6.3	Unprivileged access
CA-1994-12	8.6.7	Full system privilege
CA-1995-05	8.6.9	Full system privilege
CA-1995-13	8.7.0	Full system privilege
CA-1996-04	8.7.3	Full system privilege
CA-1996-20	8.7.5	Full system privilege
CA-1996-24	8.8.2	Full system privilege
CA-1996-25	8.8.3	Group privileges
CA-1997-05	8.8.4	Full system privilege
CA-2003-07	8.12.7	Full system privilege
CA-2003-12	8.12.8	Full system privilege
CA-2003-25	8.12.9	Full system privilege

Postfix (Secure Mailer) project

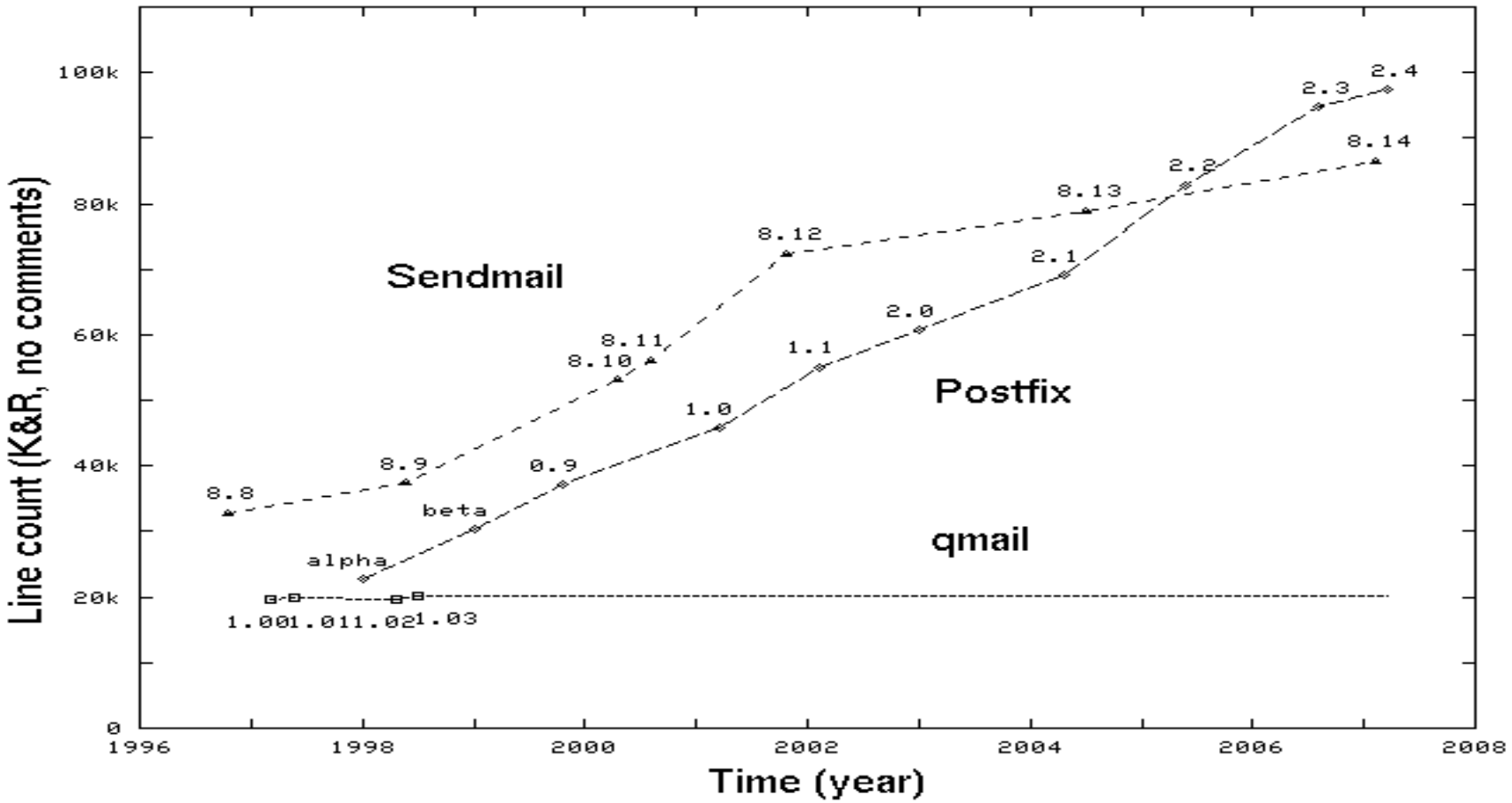
- Primary goals: more secure, easier to configure, and better performance. All primary goals were met.
- Originally developed to illustrate “secure” programming with a realistic application.
- One year after the first release, several news articles began to mention Postfix as the project that triggered IBM’s adoption of open source. Reportedly, this started when IBM’s top management saw the NY Times article.

How Postfix (Secure Mailer) helped IBM to embrace Open Source + Linux

Building up momentum

- June 1998 IBM joins the open source Apache project.
- Sept 1998 JIKES Java compiler open source release.
- Sept 1998 PKIX public key infrastructure software open source release under the name “Jonah”.
- Dec 1998 Secure Mailer open source release under the name “Postfix”. IBM’s CEO starts asking questions.
- 1999 IBM adopts Open Source and Linux strategies.

A lot has happened since then...



...even a Sendmail innovation award

MOUNTAIN VIEW, Calif. October 25th, 2006 Today at its 25 Years of Internet Mail celebration event, taking place at the Computer History Museum in Mountain View, California, Sendmail, Inc., the leading global provider of trusted messaging, announced the recipients of its inaugural **Innovation Awards**.

. . .

Wietse Venema, author, for his contribution of extending Milter functionality to the Postfix MTA.

http://www.sendmail.com/pdfs/pressreleases/Sendmail Innovation Awards_10 25 06_FINAL.pdf

Postfix lessons learned

- You can run from Windows but you can’t escape from it. Suddenly your UNIX-based mail server becomes a major vehicle for email worms and other malware.
- It’s not the spammers who destroy the infrastructure - it’s well-meaning people with ill-designed countermeasures.
- The downside of no forced upgrades: problems solved with Postfix years ago still ship with today’s operating system releases.
- Coordinated publicity can have amazing effects.

It’s not about open or closed source

“As long as there is support for ad hoc fixes and security packages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of computer system security, proper security will not be a reality.”

Roger Schell et al., “Preliminary notes on the Design of Secure Military Computer Systems”,1973.

It’s not about open or closed source

- Systems that are not built to be secure will always be like Swiss cheese, full of holes.

  You don’t make systems secure by “patching” the holes.

- How much of today’s popular systems was written before people started to worry about computer security? That is 10s of millions of lines of code.

  Security initiatives are great, but only for new systems.

- Great opportunities for firewalls, hypervisors, virtual machine monitors, and the like.

Pointers to on-line resources

- Archive of seminal papers on computer security
  http://seclab.cs.ucdavis.edu/projects/history/seminal.html
- Postfix web site, including press article archive
  http://www.postfix.org/
- TCP wrapper, SATAN, Coroner’s Toolkit, etc.
  http://www.porcupine.org/