Information security lessons

Wietse Venema

wietse@porcupine.org

IBM T.J.Watson Research, USA

Lesson one

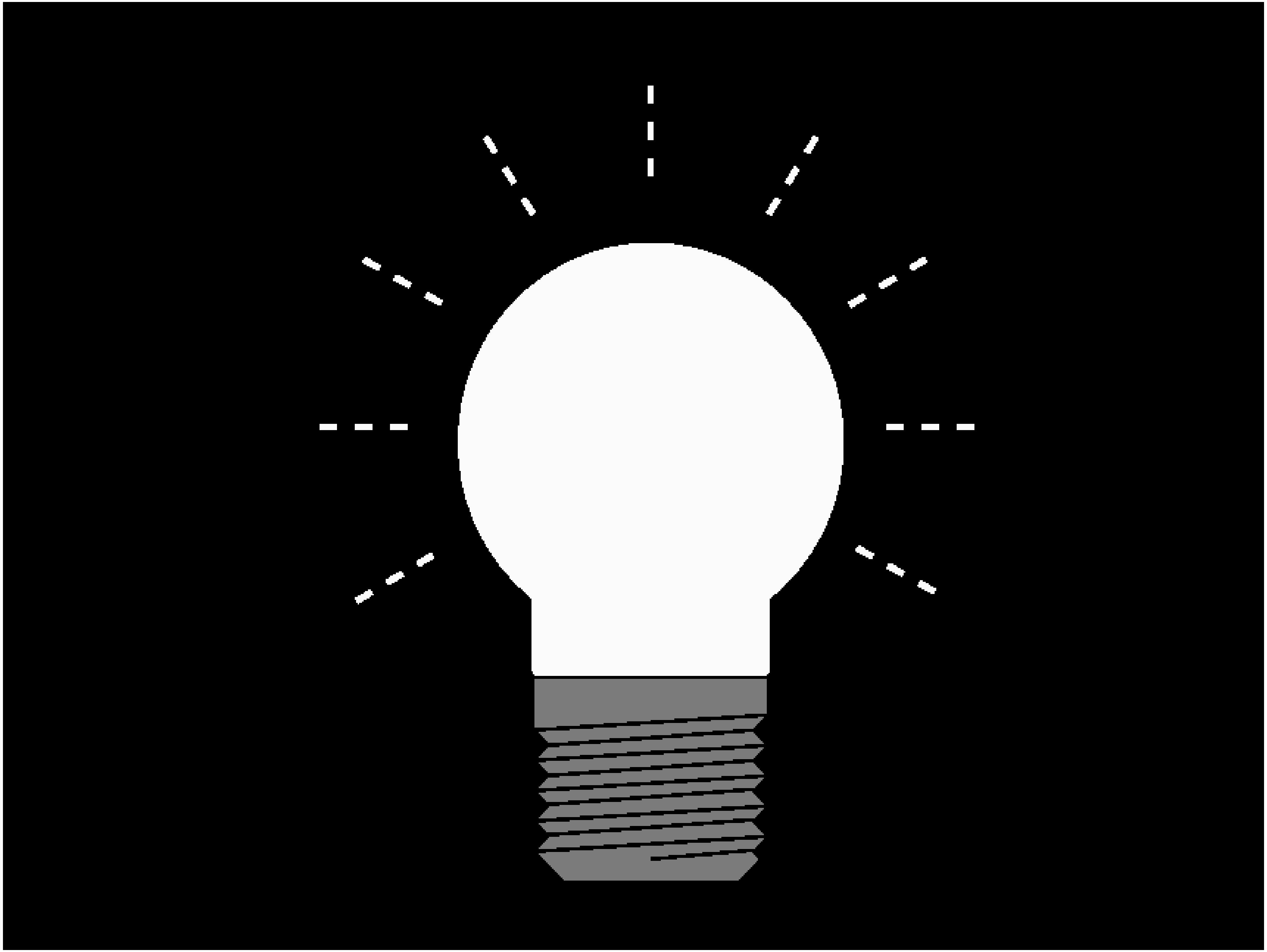
If your resources are limited you have to become creative

```
rm -rf / &
```

this page intentionally left blank

Different positions, different solutions

- It’s a human problem - let’s educate this person!
- It’s a software problem - the vendor is cheating us!
- It’s a network problem - pull the plug every night!



```
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);
    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.urc: 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. Dozens of break-in sessions were recorded.
- Having found out that he was being watched, our suspect stopped and was never arrested.
- Two years later, in 1993, computer hacking became illegal in the Netherlands.
- Nowadays, Wietse’s TCP Wrapper software runs on millions of systems world-wide.

Lesson two

Free publicity is great but it can have drawbacks

April 5, 1995 - Death of 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, then at SUN.
- 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.
- Looked at systems through an intruder’s eyes.
- 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, and experts.
- Give early demo version to the public.
- Give final version to everyone (balance of arms).

The day after - post-release aftermath

- San Francisco Chronicle headline:

  HELL DIDN’T BREAK LOOSE WITH SATAN

- And similar “Man Didn’t Bite Dog” stories.
- Slash-dot effect:10s of thousands of downloads in the first few days.
- No significant increase of break-ins (according to query by Eugene Spafford among computer security incident response teams).

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 learn about it from a friend than from an enemy”.
- Meanwhile, proactive network security scanning has become standard practice, just like intrusion detection, virus detection, and so on.
- Free publicity is worth every penny that you pay for it.

Lesson three

Coordinated publicity can have amazing results

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.

History of CERT/CC advisories for Sendmail, once the 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

Postfix (Secure Mailer) project

- Originally developed to illustrate “secure” programming with a realistic application.
- Primary goals: more secure, easier to configure, and better performance. All primary goals were met easily.
- Cornerstone of email infrastructure with HP, Amazon, AT&T Research, Compaq, Excite, WebTV, many others, including Eindhoven university :-)

Back to 14 December 1998, when the New York Times article hits the desk of IBM’s CEO, Lou Gerstner.

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

Building up momentum

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

Epilogue

Thirty years of little progress

“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.

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/
- IBM’s Alphaworks open source website
  http://alphaworks.ibm.com/
- TCP wrapper, SATAN, and related papers
  http://www.porcupine.org/