Welcome to

IT Kick Off 2019

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

bella-center-jan-2019.tex in the repo security-courses

Happy New Year 2019 - same problems

Who am I

- Master in computer science from University of Copenhagen
- Got interested in internet security around early 1990s reading the Morris Internet worm analysis
- Began reading a lot, there was no IT-security education except a bit of cryptography
- Today white-hat hacker, security consultant, internet samurai
  does security testing - penetration testing
- Teach a lot - 2019 Diploma in IT-Security KEA Kompetence, starts february
  This education is new only existed for about 3 years and is needed
- Keywords: network and security, internet technologies, network packets

We are all part of security

Internet Security a Short Story

Early internet before 1980 - Universities, mail was the popular *app*

TCP/IP 1980s - got IP/TCP around 1983

Systems were big servers VAXEN

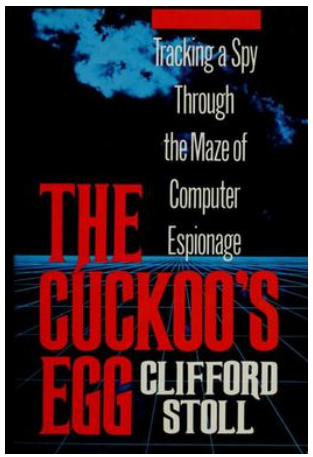
Around 60.000s servers connected on the internet by 1988

Security was not a high priority, research and development

Two examples from history

- Cuckoo's Egg 1986 A real spy story
- Morris Internet Worm, On the evening of 2 November 1988
  The Internet Worm Program: An Analysis
  Purdue Technical Report CSD-TR-823, Eugene H. Spafford

Cuckoo's Egg 1986 A real spy story



Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Clifford Stoll

During his time at working for KGB, Hess is estimated to have broken into 400 U.S. military computers

Source: `https://en.wikipedia.org/wiki/Markus_Hess`

Morris Internet Worm - 30 years ago

Used multiple vulnerabilities:

- Sendmail Debug functionality, we have similar things and Google Hacking
- Buffer overflow in fingerd, we still have those
- Weak passwords/password cracking, list of 432 words and /usr/dict/words, same problem today
- Trust between systems rsh, rexec, think Domain Admin today
- Found new systems using /etc/hosts.equiv, .rhosts, .forward, netstat ...

Also known as the Morris Internet Worm

The Internet Worm Program: An Analysis
Purdue Technical Report CSD-TR-823, Eugene H. Spafford

Resulted in creation of the CERT, `http://www.cert.org`

Internet Worms history repeats itself

Camouflage, tried to hide, malware today hides as well

- Program name set to 'sh', looks like a regular shell
- Used fork() to change process ID (PID)
- Worms in the 2000s spread quickly, like Code Red 2001 to approx 350.000 systems in a week
- SQL Slammer "It spread rapidly, infecting most of its 75,000 victims within ten minutes."

New malware today can use the same strategies

Except a lot of malware tries to stay hidden, less noisy

Using a small password list of 50 words it is possible to create your own botnet with 100.000s

Source: `https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms`

Hackers don’t give a shit

Your system is only for testing, development, ...

Your network is a research network, under construction, being phased out, ...

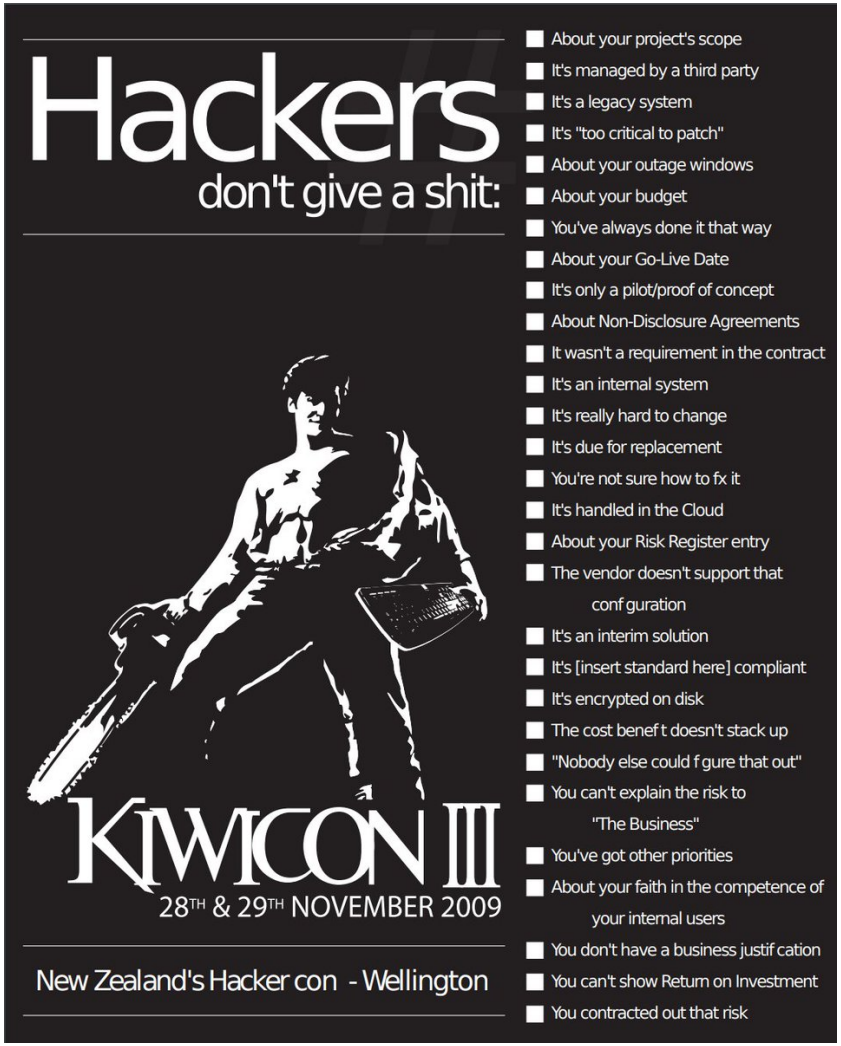
Try something new, stay aware

Bring all the exceptions forward, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Make sure to alert someone if something is strange

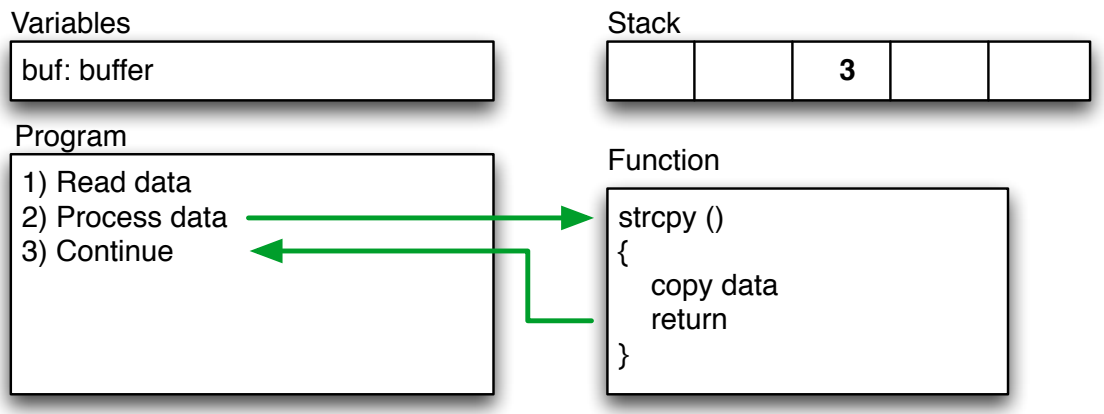
if something can become a threat

May need to repeat this multiple times, until fixed



Buffer Overflows - normal programs

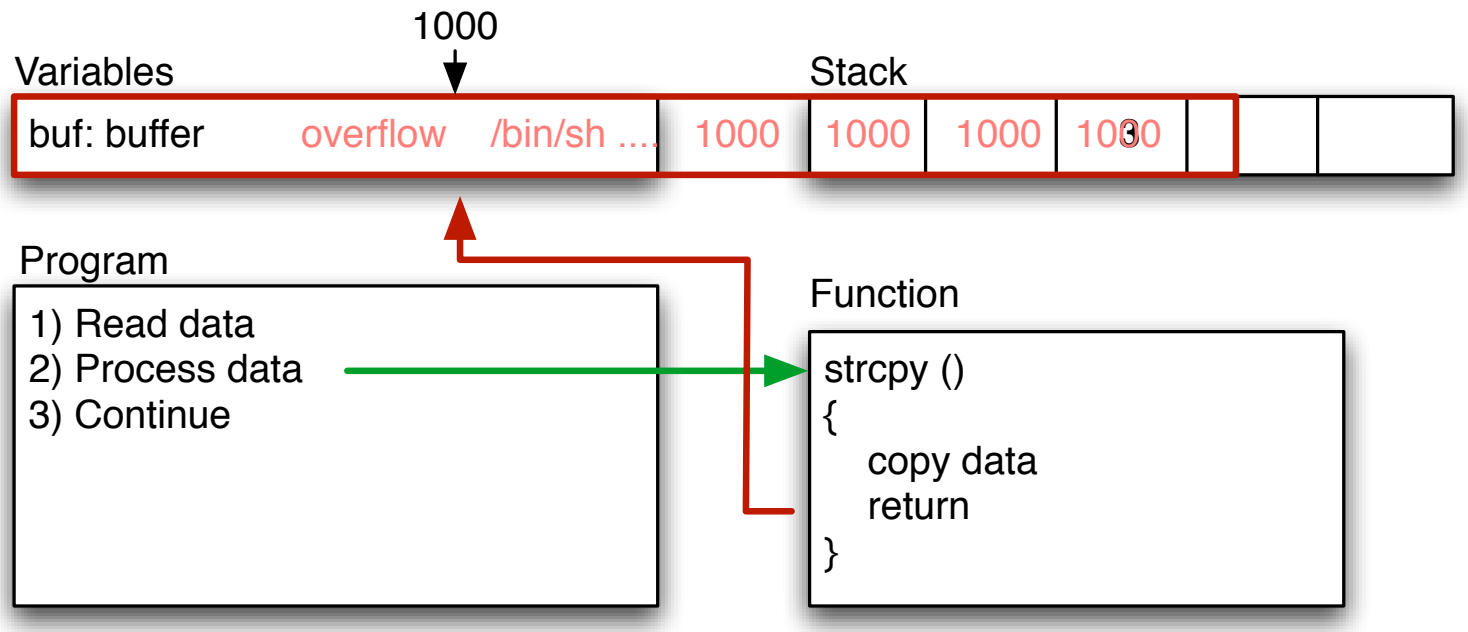
How do attacks even work?




```
main(int argc, char **argv)
{       char buf[200];
         strcpy(buf, argv[1]);
         printf("%s\n",buf);
}
```

All programs have flaws

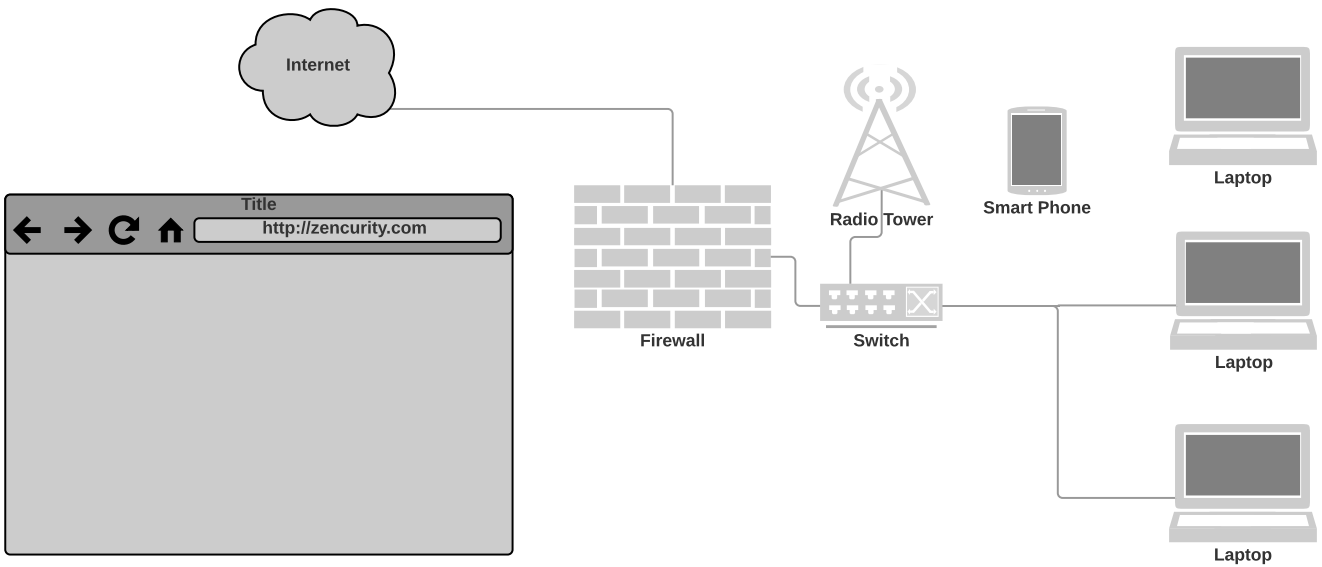
Buffer Overflows - bad programs



Using LARGE input with shell code

Software written many years ago, and never updated - are probably even more insecure, isolate, replace, phase out

Your Privacy under Attack



- Your data travels far
- Often crossing borders, virtually and literally
- Many technologies are old and insecure

Data found in Network data

Lets take an example, DNS

Domain Name System DNS breadcrumbs

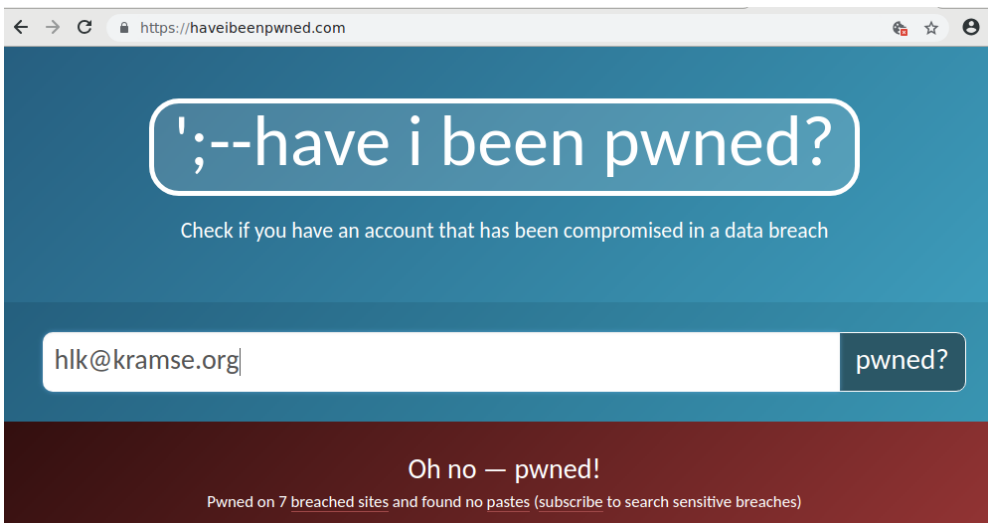
- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit
- Privacy issue - how to monitor company without invading employee privacy

Advice show your users,ask them to participate in a experiment

Join this Wireless network SSID and we will show you who you are on the internet

Maybe use VPN more - or always!

Your data has already have been owned by criminals



Your data is already being sold, and resold on the Internet

Stop reusing passwords, use a password safe to generate and remember

Check you own email addresses on `https://haveibeenpwned.com/`

Go ahead try the web site - hold up your hand if you are in those dumps

Recommendations - Comply Everywhere, Act Anywhere

Follow company guidelines, be skeptical, stop and think

Then take control of your own security

Laptop storage must be encrypted

Firewall must be enabled

Suggestions

- Write an email to everyone in your organisation:
  "Hi All, we need to identify systems without full disk encryption
  - come see us, we have christmas cookies left, Best regards IT"

I like your 2 Feet Principle, direct surroundings

Keep reporting phishing attempts, attempted breakins etc.

Imagine Attacks from the Inside

- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
  NotPetya cost Maersk about 1.9 billion DKK
- entry thought to be via software update of M.E.Doc [uk] an Ukrainian tax preparation program
- Attackers are very creative and have a large attack surface to most companies

Various key attack types, clients and employees

- Phishing - sending fake emails, to collect credentials
- Spear phishing - targetted attacks
- Person in the middle - sniffing and changing data in transit
- Drive-by attacks - web pages infected with malware, often ad servers
- Malware transferred via USB or email
- Credential Stuffing, Password related, like re-use of password, see slide about being pwned

If we all wait a bit, and not click links immediately

Hackers try to create ”urgency”, click this or loose money

Overlapping Security Incidents

New data breaches nearly every week, these from danish news site `version2.dk`

Problem, we need to receive data from others

Data from others may contain malware

Have a job posting, yes
- then HR will be expecting CVs sent as .doc files

or the other way

Attackers used a LinkedIn job ad and Skype call to breach bank's defences

The attack

One of these is the Chilean news site's claim that the attack started with a LinkedIn advert offering a developer role to which a Redbanc employee replied.

The attackers set up a Skype call to conduct an interview during which the individual was tricked into downloading a file called ApplicationPDF.exe, sent via a weblink, which subsequently infected the employee's computer.

https://nakedsecurity.sophos.com/2019/01/21/attackers-used-a-linkedin-job-ad-and-skype-call-to-breach-banks-defences/

Questions?

Henrik Lund Kramshøj hlk@zencurity.com

Need help with infrastructure security or pentesting, ask me!

You are always welcome to send me questions later via email