



Welcome to

White Hat Hacking, protect your network

Bella Center 2019

Henrik Lund Kramshøj hlk@zecurity.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, pentester, security consultant, internet samurai
- Teach a lot - 2019 Diploma in IT-Security KEA Kompetence, starts february
- Keywords: network and security, internet technologies, network packets, BGP
- **We need more people in IT-security**



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

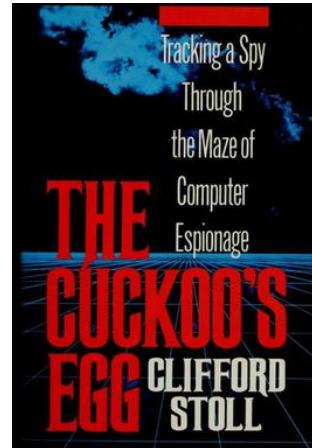
Security was not a high priority, research and development

- Cuckoo's Egg 1986
- 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



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, go to your management

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

Think like attackers - don't hold back

Ask for permission before you go full monty

Hackers don't give a shit:



KIWICON III
28TH & 29TH NOVEMBER 2009

New Zealand's Hacker con - Wellington

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

Try something new

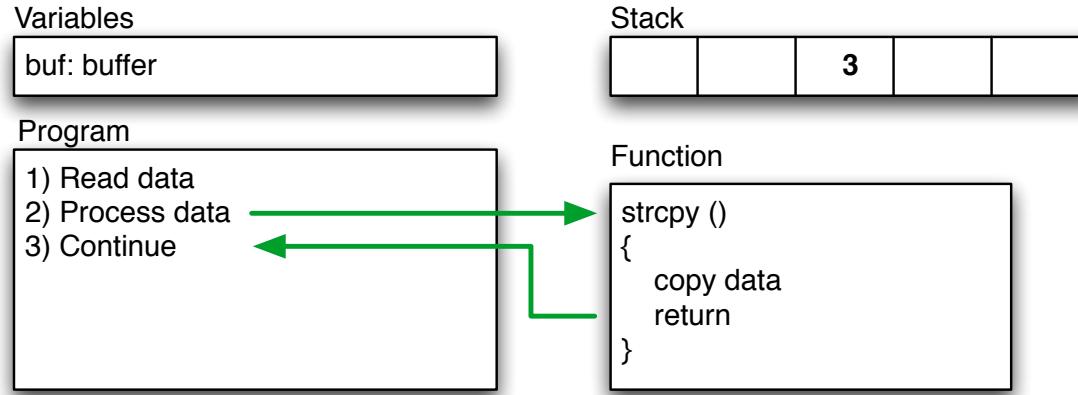


Do you think like an attacker?

Why not.

- This talk will try to convince you to start attacking yourself, your company, your life.
- Start using Nmap, Wireshark, Kali Linux
- Learn some hacking skills, so you can recognize bad and insecure design

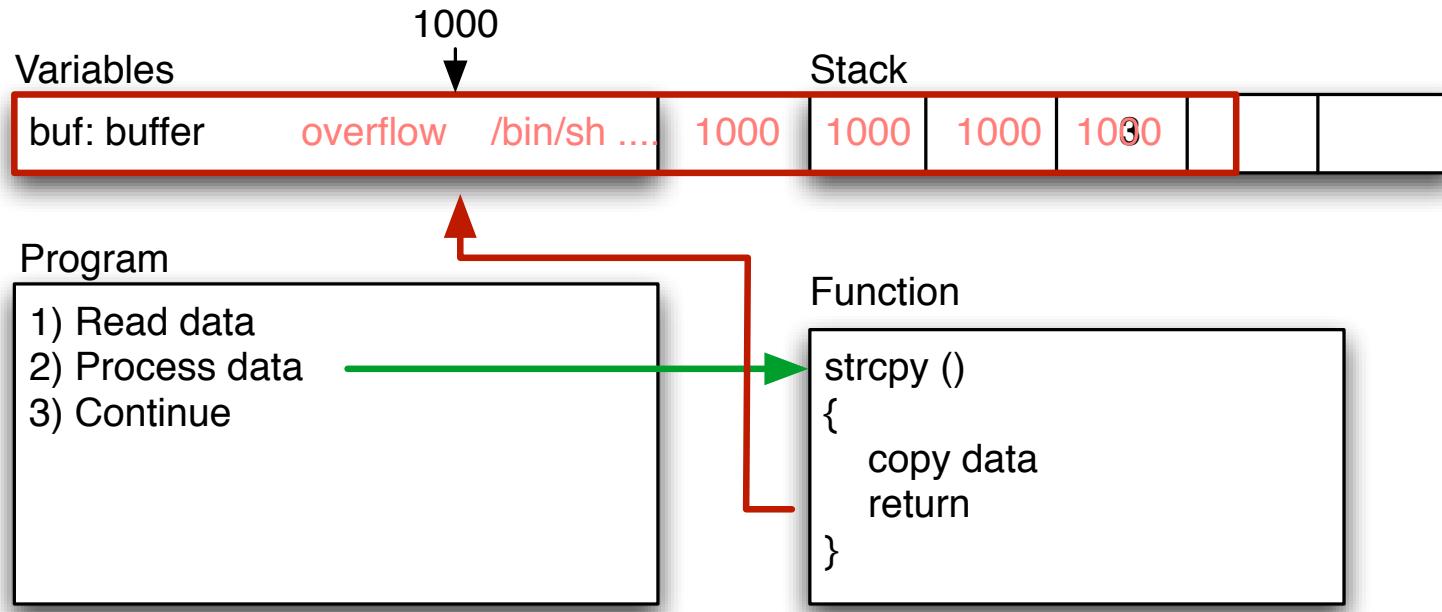
Buffer Overflows - normal programs



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

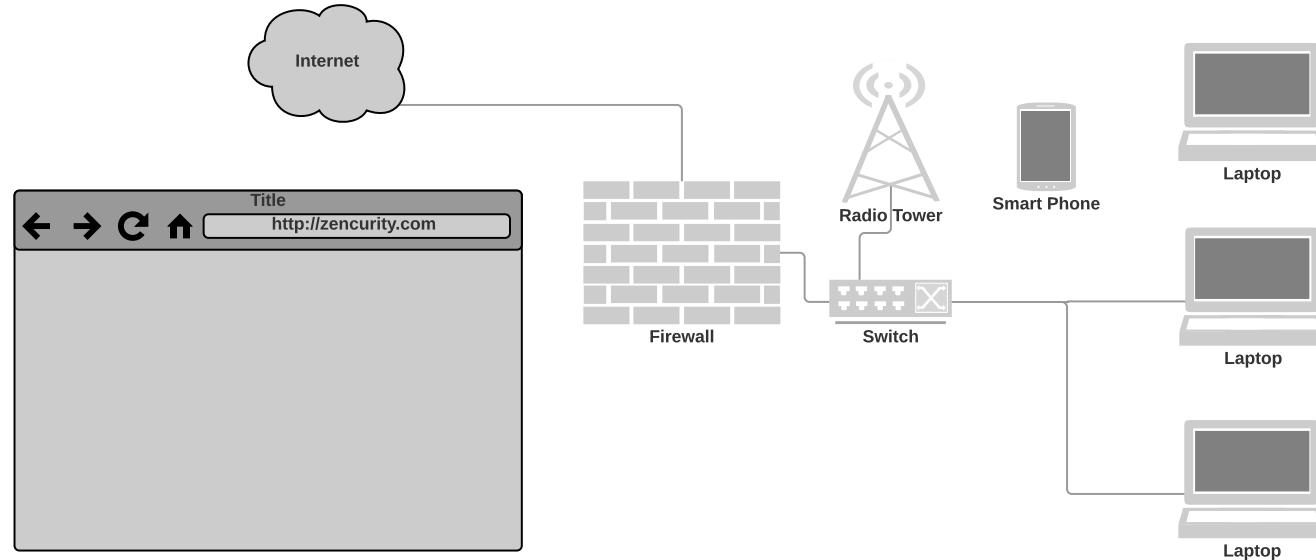
All programs have flaws

Buffer Overflows - bad programs



Using LARGE input with shell code

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

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!

You already have been pwned



A screenshot of a web browser displaying the Have I Been Pwned? website at <https://haveibeenpwned.com>. The page has a teal header with the text ':;--have i been pwned?' in white. Below the header is a sub-header: 'Check if you have an account that has been compromised in a data breach'. A search bar contains the email address 'hlk@kramse.org'. To the right of the search bar is a dark blue button labeled 'pwned?'. Below the search bar, a large red banner displays the message 'Oh no — pwned!' in white. Underneath the banner, smaller text reads 'Pwned on 7 breached sites and found no pastes (subscribe to search sensitive breaches)'. The overall design is clean and modern.

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

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

Check your own email addresses on <https://haveibeenpwned.com/>

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

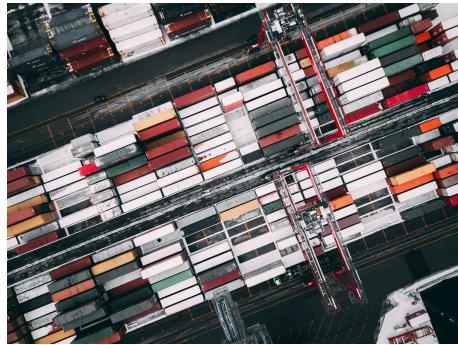
- Write an email to everyone in your organisation:
"Hi All, we need to identify systems without full disk encryption
- come see us, we have christmas cookies left, Best regards IT"



I like your 2 Feet Principle, direct surroundings

Keep reporting phishing attempts, attempted breakins etc.

Start Attacking from the Inside



- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
Having a large open network may cost you 1.9 billion DKK - ref Maersk
- Try scanning everything, start in a small corner, expand
- Scan all your danish segments, one by one, then the nordic, then the world
- Yes, things may break - FINE, BREAKING is GOOD

Better to break while we are ready to un-break

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