Hacking in C

About this course: topics & goals

- Standard ways in which software can be exploited
  - understanding how such attacks work
  - understanding what makes these attacks possible
  - doing some attacks in practice

- Root cause analysis: why are things so easy to hack?

- This involves understanding
  - **programming languages**, compilers, and operating systems, and the **abstractions** that they provide
  - the languages, **representations**, and interpretations involved
  - the potential for trouble – in the form of software vulnerabilities - all this introduces

Hacking in C

- security problems in machine code compiled from C(++) source code running on standard CPU and operating system.

- to understand this, we need to know how
  - the data representations involved
  - the memory management that the programmer has to do

Prerequisites

- **Imperatief Programmeren**
  - we won't use C++, but C
  - biggest change: using **`printf`** instead of **`>>`** ?

- **Processoren**
  - what is the functionality that a typical CPU offers, on which we have to run our software written in higher-level languages?

    Eg. fetch-execute cycle of the CPU, with Program Counter (PC) registers where in the code we are, which is modified for a JUMP instruction and incremented for the other instructions

Lectures & lab sessions

- Lectures Mondays 13:45-15:30 in HG00.304
- Lab sessions Thursdays 10:45-12:30 in HG00.137 & HG00.625

Aanstaande woensdag: als je al bekend met Linux command line ga dan naar HG00.625

- All course material will be on
  http://www.cs.ru.nl/~erikpoll/hic

Lab exercises

Weekly lab session with weekly programming/hacking exercise

- *Exercises to be done in pairs*
- *Doing the exercises is **obligatory** to take part in the exam;*
- *Exercises will be lightly graded to provide feedback,*
  *with **nsi-regeling**:*
  you can have only one exercise niet-serieus-ingeleverd

- You learn stuff in the exercises that you won't learn at the lectures, and vv.
- Beware: exercises of one week will build on knowledge & skills from the previous week
- Also: turning up for the lab sesions might be *crucial* to sort out practical problems (with C, gcc, Linux, ...)

Lab exercises

We use

- C as programming language, not C++
- Linux from the command line aka shell
- the compiler gcc

So no fancy graphical user interfaces (GUIs)
for the operating system (OS) or the compiler

Why?

- GUIs are nice, but *hide* what OS and compiler are doing
- the command line is clumsy at first,
  - using commands instead of pointing & clicking

  but gives great power
  - we can write shell scripts: programs that interact with the OS

‘to hack’

NB several meaning and connotations, incl.

1. To write software in a clever way
   – to really exploit all the capabilities a system offers

2. To break into a computer system.

3. To fix some problem in a quickly & ugly way

Focus of this course 1 & 2.

How do you break into a computer system?

1. Using user credentials – username/password

   How do you get those?

   – *default passwords*

Default passwords exploited by Mirai botnet

USER:	PASS:
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
guest	12345

USER:	PASS:
admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	00000000
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	fucker

Default passwords exploited by Mirai botnet

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

How do you break into a computer system?

1. Using **user credentials** – username/password

   How do you get those?

   – *default passwords*
   – *phishing*
   – *brute forcing*
   – *eavesdropping,*
      • *on unsecured network connection,*
      • *with keylogger hardware or software keylogger*
   – *using stolen password files*
      • *which may need to be brute forced, if passwords are hashed*
   – *...*

2 Using **flaws in the software**

   – Focus of this course & web security next quarter

Security problems in software

Terminology can be confusing:

(security) weakness, flaw, vulnerability, bug, error, coding defect, ...

Important distinction:

1. security **weakness/flaw:**

   something that is wrong or could be better

2. security **vulnerability**

   weakness/flaw that can actually be exploited by an attacker,

   This requires the flaw to be

   1. *accessible - attacker has to be able to get at it*
   2. *exploitable – attacker has to be able to do some damage with it*

Eg by unplugging your network connection, many vulnerabilities become flaws

Warning: there is no standardised terminology for the distinction above!

Software security prices (2015)

design vs implementation flaws

Software vulnerabilities can be introduced at different “levels”

- design flaws
  - fundamental error in the design
- implementation flaws or coding error
  - introduced when implementing

focus of this course

The precise border is not precise

it can be debatable whether a flaws is a design or implementation flaw

To understand implementation flaws, we need to look 'under the hood' of how a programming language works

To understand implementation flaws