Operating Systems Security And Why It (Mostly) Doesn't Matter

Patrick Hof - RedTeam Pentesting GmbH
patrick.hof@redteam-pentesting.de
https://www.redteam-pentesting.de/

Radboud University, Nijmegen, 19 December 2016

RedTeam Pentesting, Dates & Facts

- Founded in 2004 at RWTH Aachen University
- 9 penetration testers
- Conducting penetration tests world-wide
- Specialisation exclusively on penetration tests

Pentest – Introduction

- Targets and attacker-model defined in preliminary meeting
- Conducted from the attacker's perspective
  → Same methods as “bad guys”
- Individualised search for security vulnerabilities
- Detailed documentation

Data Breaches 2016

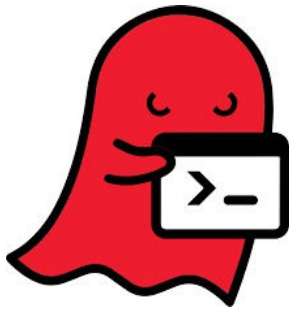
- If you look at the security-related headlines in 2016, we're pretty much doomed
- Large data breaches 2016 (just to name a few):
  - Dec 14th, Yahoo: More than 1B(!) user accounts (from August 2013)
  - Nov 23rd, AdultFriendFinder: 421M user accounts
  - Sep 2nd, Dropbox: 68M user accounts (from 2012)
  - May 17th, LinkedIn: 117M user accounts (from 2012)
  - and the list goes on...[1]

[1] Source: https://www.identityforce.com/blog/2016-data-breaches

Branded Security Vulns

We even have logos now! Finally, people will understand the severity of the situation!

CVE-2016-5195



CVE-2015-0235

CVE-2016-0800

CVE-2014-6271

CVE-2016-3714

CVE-2014-0160

Security Incidents Wherever You Look

- Why do we see so many incidents?
- There seem to be more security-related incidents than ever
- In our pentests, we usually can achieve what we agreed before should not happen, why is that?

I tried to find the cheesiest image I could get…

Defense Mechanisms Are Getting More Advanced

- IDS/IPS
- Traffic analysis up to application layer
- Antivirus
- Security appliances combining all of the above
- Operating systems security (ASLR, DEP/NX etc.)
- 2FA
- Centralized security, e.g. group policies on Windows
- ...

Investments in IT Security are Rising

- When we started 10 years ago, “pentests” were not widely known
- Now, companies are investing more than ever in IT security (search for “Hot Cybersecurity Stocks 2016” on Google, I dare you)
- Shouldn't this reduce the amount of incidents?

Why so Many Incidents?

Ok, so maybe things are not as bad as I make it look like.

Why so Many Incidents?

- Theory: Working as a pentester only shows very vulnerable companies, everyone else is secure and therefore doesn't do pentests.

Why so Many Incidents?

- Theory: Working as a pentester only shows very vulnerable companies, everyone else is secure and therefore doesn't do pentests.
- Answer: No, those who do pentests are rather security-aware, otherwise they wouldn't bother.

Why so Many Incidents?

- Theory: The media are giving a skewed view on things for the sake of making scary headlines about “the cybers”, therefore making it seem worse than it actually is.

> “*So we have to get very, very tough on cyber and cyber warfare. It is a, it is a huge problem. I have a son. He's 10 years old. He has computers. He is so good with these computers, it's unbelievable. The security aspect of cyber is very, very tough.*
>
> – Abraham Lincoln ”

Why so Many Incidents?

- Theory: The media are giving a skewed view on things for the sake of making scary headlines about “the cybers”, therefore making it seem worse than it actually is.
- Answer: Might be partly true, but apart from the usual media sensationalism, many hacks are real. We do see a lot of vulnerable systems in our work and we also get feedback from clients about breaches they had that were never reported to anyone.

Why so Many Incidents?

- Theory: There is so much money in the security industry that everyone is interested in scaring people into buying as much “security” as possible.

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
F 23214550 K
WASHINGTON, D.C.

Why so Many Incidents?

- Theory: There is so much money in the security industry that everyone is interested in scaring people into buying as much “security” as possible.
- Answer: Partly true, there's a lot of very questionable stuff out there that makes millions in profits, but as I already said: we do see a lot of very insecure systems in our work, and if you look at the recent security research, others do too.

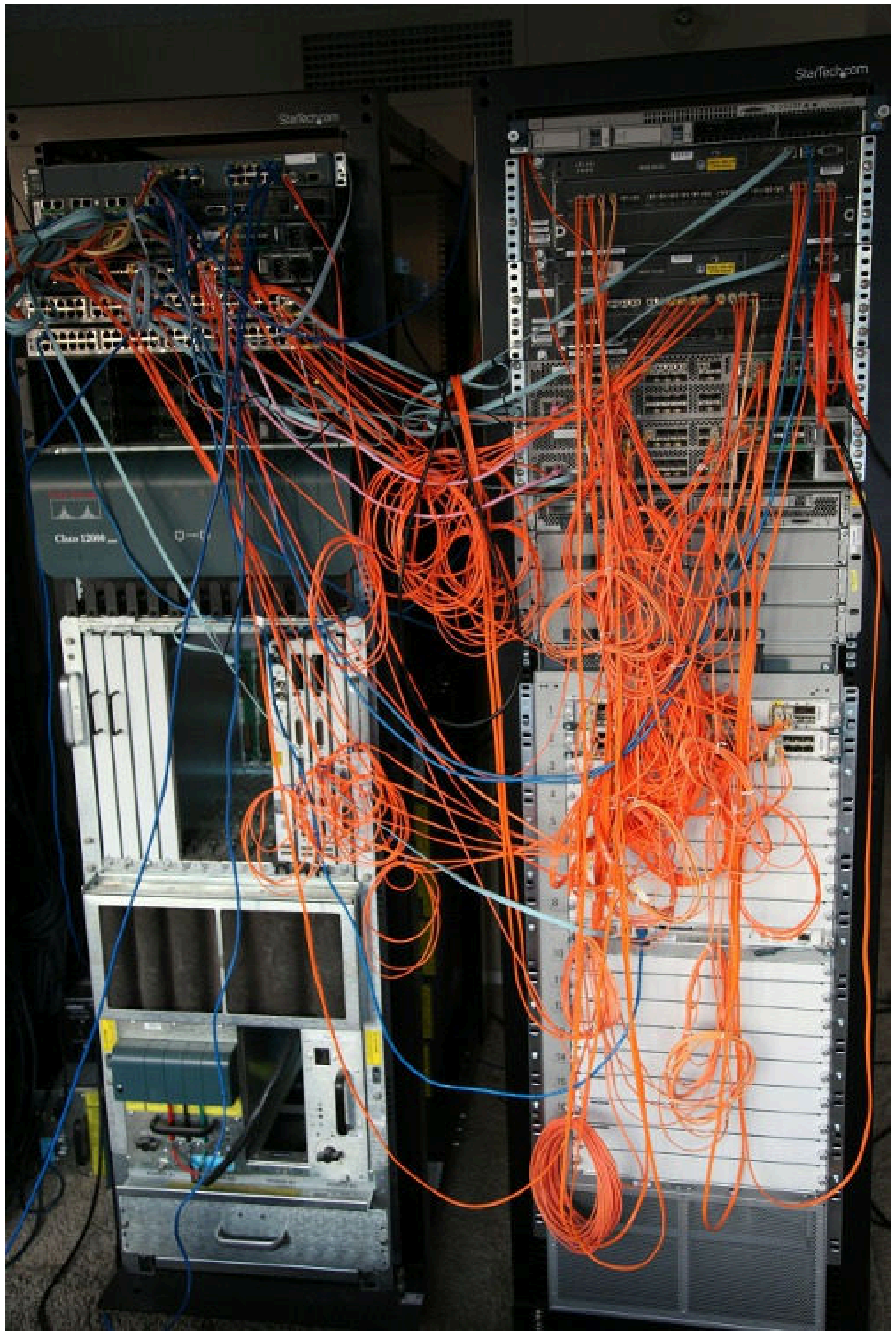
The Real Problems

Some ideas what the real problems could be:

- Everything is online these days, or in the process of going online: Banking, shopping, social interaction...
- IT is more and more prevalent in every company, (almost) nobody works without IT or the Internet
- Employees should be able to work from anywhere (and be available 24/7), so remote access is needed even from private hardware (BYOD)
- Things change fast, companies are trying to keep up with the latest trends
- There is a huge market for cheap gadgets and the "Internet of Things"

The Real Problems

- Complexity breeds bugs, bugs are vulnerabilities waiting to be exploited
- Companies add more features instead of securing the already available
- Attackers are interested in data, not necessarily a root shell



The Real Problems

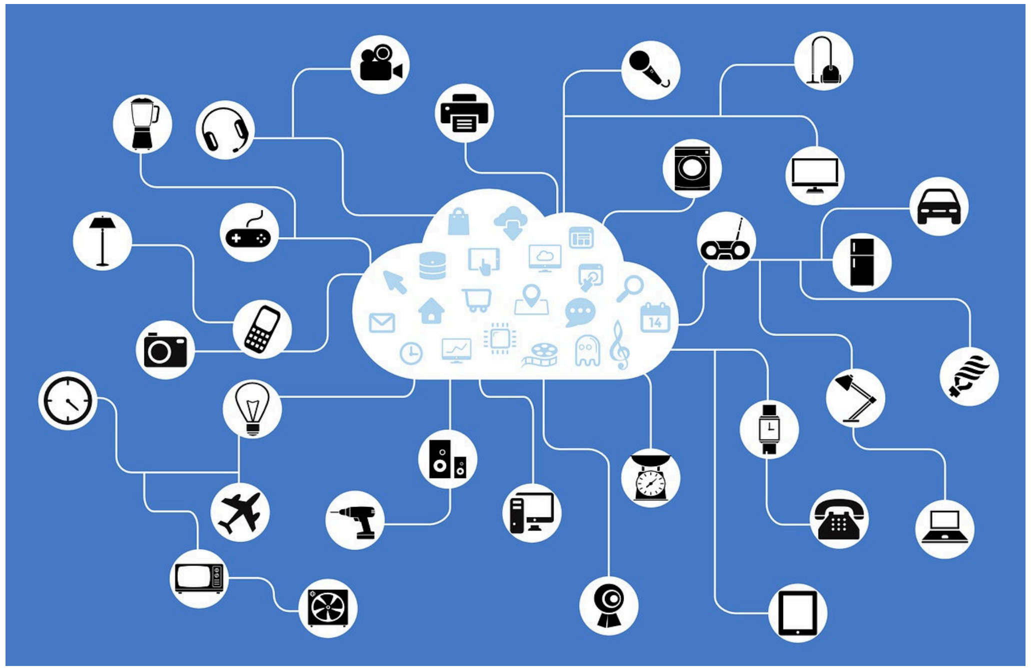
- Malvertising: Ad networks currently have a huge malware problem
- Content Delivery Networks (CDN):
  - One hack, millions of victims
  - Hide behind the "big name" when delivering malware
- JavaScript bloat
  - March 2016: The "left-pad fiasco"[1]: 2.486.696 downloads in February alone for a module that left-pads strings!
  - Again: hack one developer, target *loads* of applications

[1] http://www.haneycodes.net/npm-left-pad-have-we-forgotten-how-to-program/

The Real Problems

More Buzzwords:

- Internet of Things (IoT)
- The Cloud
- Antivirus
- Smartphones



Example: Home Routers

9.12.2016: Netgear, 8 models can be exploited like it's '99:

```
http://<router_IP>/cgi-bin/;COMMAND
```

- This is how I exploited my Linksys WRT54G Wi-fi router to install Linux, in 2002! Even then, command injections were already a well-known vulnerability.
- There are exploit kits used by malvertisers to open up home routers with vulnerabilities like this one.

Example: Antivirus

- Antivirus software is often indistinguishable from a kernel root kit
- Embeds itself deeply into the system, hooking kernel functions
- Check out Tavis Ormandy's work at Google Project Zero
  - Exploits for Symantec and Norton, Avast, Trend Micro...
- Recent research (12.12.2016) by Andrew Fasano: McAfee Virus Scan for Linux, 10 vulnerabilities that can be chained to achieve remote command execution as root[1]

[1] https://nation.state.actor/mcafee.html

Example: Serialization Considered Harmful

- Problem: Transparently sending objects back and forth blurs the distinction between untrusted client and trusted server for programmers
- One of the newer tools (released 2015): `ysoserial`[1]

```
ObjectInputStream.readObject()
  AnnotationInvocationHandler.readObject()
      [...]
                Runtime.getRuntime()
            InvokerTransformer.transform()
              Method.invoke()
                Runtime.exec()
```

[1] https://github.com/frohoff/ysoserial

What Else?

Operating Systems Security: Mostly Post Exploitation

aka: we already got the data, but while we're at it...

Operating Systems Security: Windows

- In many cases: Once you are part of the domain, it is just a matter of time until you are domain admin
- Get local user hashes/tickets from memory
- If not already domain admin: Access other machines with credentials/hashes/tickets found until you have a domain admin account
- Game over, connect to domain controller and create for example a golden ticket
- `mimikatz`[1] implements all this

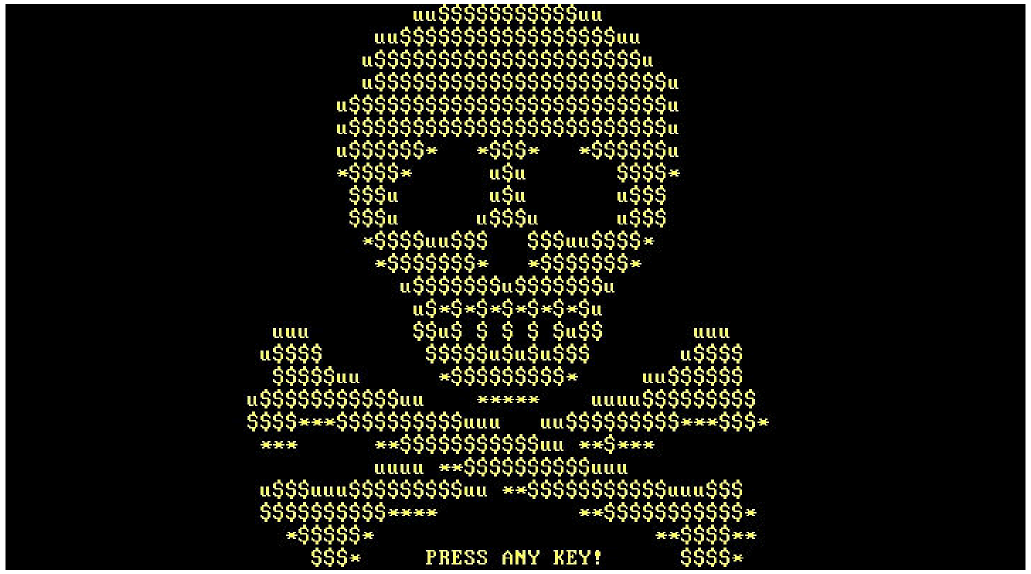
[1] https://github.com/gentilkiwi/mimikatz

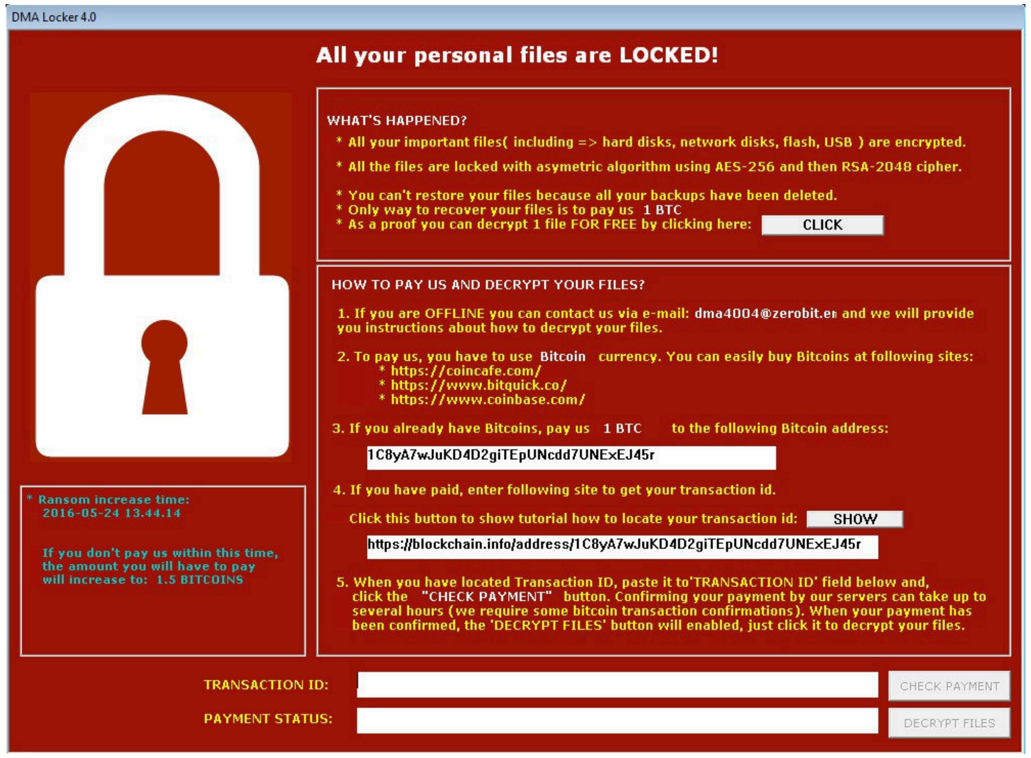
Operating Systems Security: Linux

- Linux is found mostly on servers
- There, you have the usual problem: Only few install their patches on time
  → Outdated kernel, glibc etc.
- Use local privilege escalation to get root
- More fragmented, rather individual how you can get access to more systems
- E.g. passwords in the `.bash_history`, private SSH keys, weak passwords, open shares, config files with credentials...

Are We Really Doomed?

- We start to see that consumers demand security, but only when it hurts (e.g. Ransomware)
- Nobody cares if they're part of a botnet, everyone cares if their family photos are encrypted (or for companies: their precious Excel reports)





All your personal files are LOCKED!

WHAT'S HAPPENED?

* All your important files(including => hard disks, network disks, flash, USB) are encrypted.
* All the files are locked with asymetric algorithm using AES-256 and then RSA-2048 cipher.

* You can't restore your files because all your backups have been deleted.
* Only way to recover your files is to pay us 1 BTC
* As a proof you can decrypt 1 file FOR FREE by clicking here: CLICK

HOW TO PAY US AND DECRYPT YOUR FILES?

1. If you are OFFLINE you can contact us via e-mail: dma4004@zerobit.en and we will provide you instructions about how to decrypt your files.

2. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
   * https://coincafe.com/
   * https://www.bitquick.co/
   * https://www.coinbase.com/

3. If you already have Bitcoins, pay us 1 BTC to the following Bitcoin address:
   1C8yA7wJuKD4D2giTEpUNcdd7UNExEJ45r

4. If you have paid, enter following site to get your transaction id.
   Click this button to show tutorial how to locate your transaction id: SHOW
   https://blockchain.info/address/1C8yA7wJuKD4D2giTEpUNcdd7UNExEJ45r

5. When you have located Transaction ID, paste it to'TRANSACTION ID' field below and, click the "CHECK PAYMENT" button. Confirming your payment by our servers can take up to several hours (we require some bitcoin transaction confirmations). When your payment has been confirmed, the 'DECRYPT FILES' button will enabled, just click it to decrypt your files.

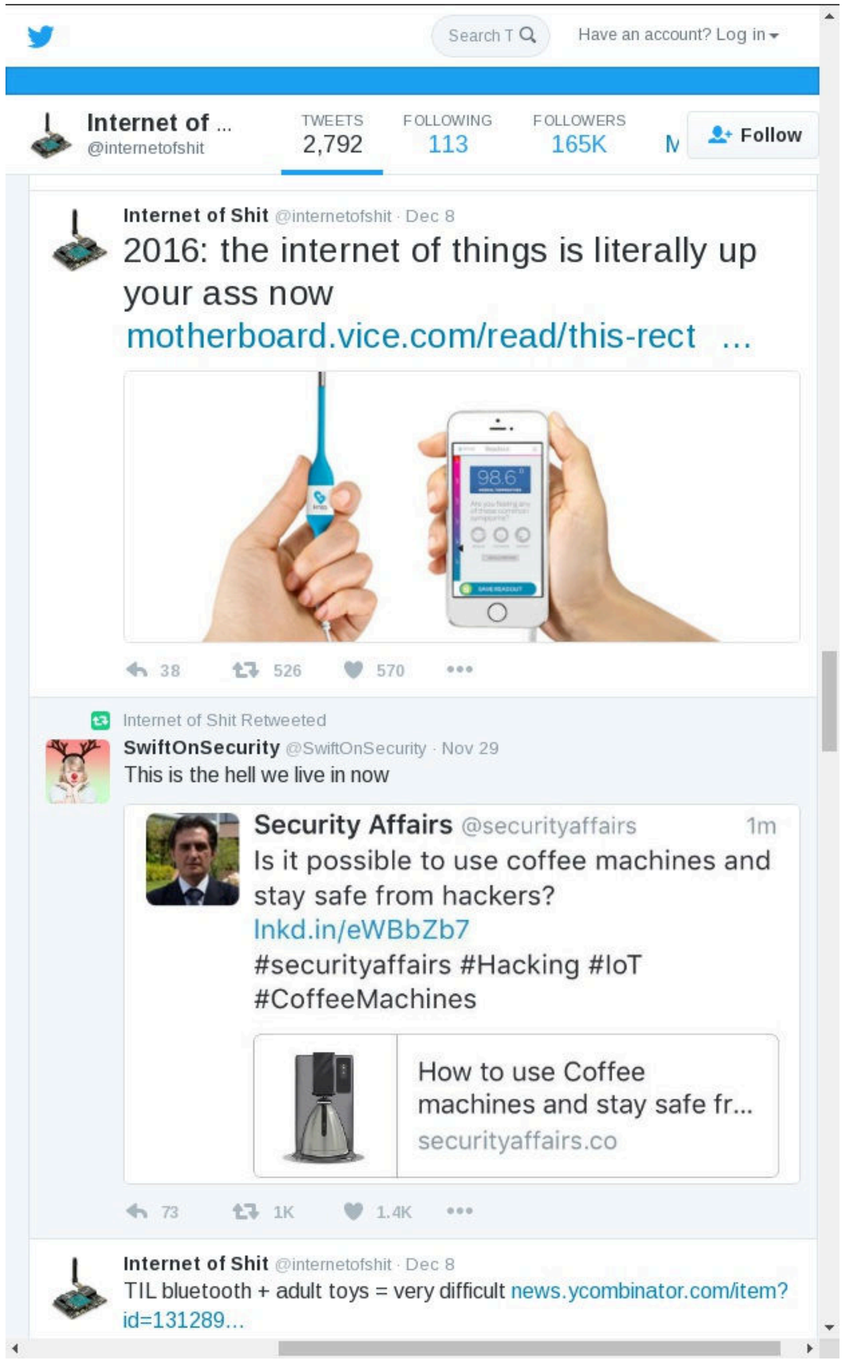
* Ransom increase time:
2016-05-24 13.44.14

If you don't pay us within this time, the amount you will have to pay will increase to: 1.5 BITCOINS

TRANSACTION ID: CHECK PAYMENT
PAYMENT STATUS: DECRYPT FILES

Are We Really Doomed?

- Reduce complexity (KISS) instead of increasing it
- Make security part of the development cycle
- Patch your systems regularly!
- Not everything needs to be connected to the Internet



Internet of ... @internetofshit

TWEETS 2,792 FOLLOWING 113 FOLLOWERS 165K

Internet of Shit @internetofshit · Dec 8
2016: the internet of things is literally up your ass now
motherboard.vice.com/read/this-rect ...

38 526 570

Internet of Shit Retweeted
SwiftOnSecurity @SwiftOnSecurity · Nov 29
This is the hell we live in now

Security Affairs @securityaffairs 1m
Is it possible to use coffee machines and stay safe from hackers?
lnkd.in/eWBbZb7
#securityaffairs #Hacking #IoT #CoffeeMachines

How to use Coffee machines and stay safe fr...
securityaffairs.co

73 1K 1.4K

Internet of Shit @internetofshit · Dec 8
TIL bluetooth + adult toys = very difficult news.ycombinator.com/item?id=131289...

Questions?

Thank you for listening!