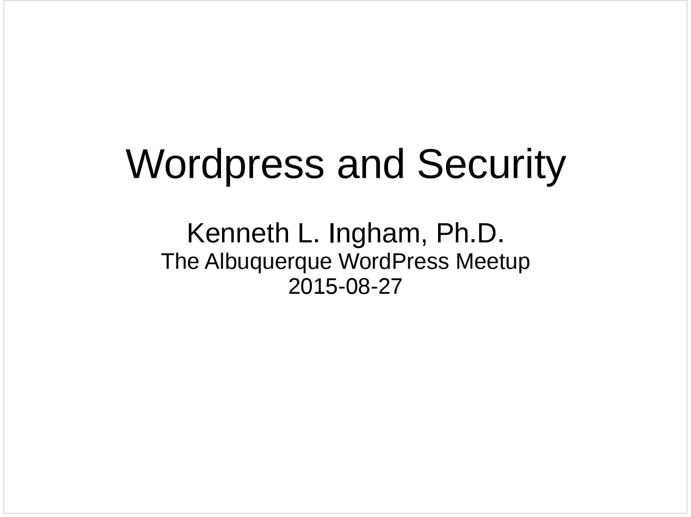
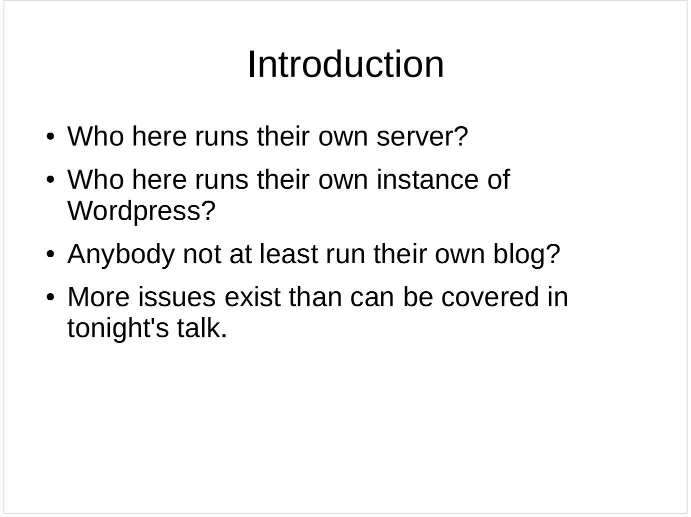


Wordpress and Security

Kenneth L. Ingham, Ph.D.
The Albuquerque WordPress Meetup
2015-08-27



Introduction

- Who here runs their own server?
- Who here runs their own instance of Wordpress?
- Anybody not at least run their own blog?
- More issues exist than can be covered in tonight's talk.

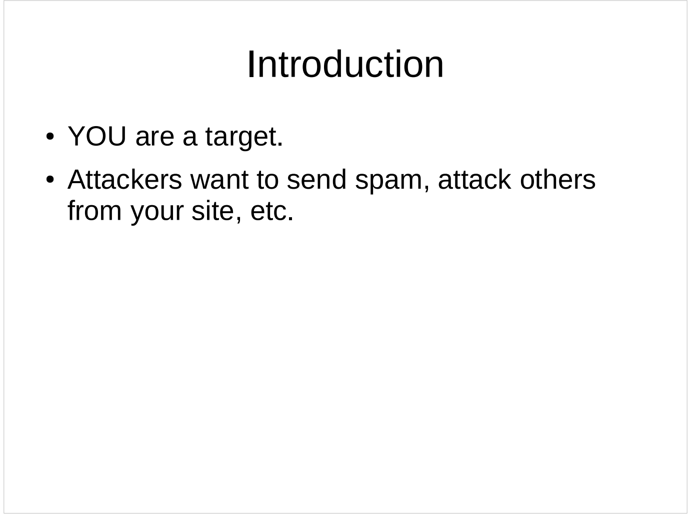
My background
PhD in CS in security
Work primarily with developers on producing more secure software
Professional photographer, earning 1/3 to ½ of my income this way
Three blogs, two more active than the third

Introduction

- >70% of WordPress installations are vulnerable to attacks
- total number of hacked WordPress websites in 2012 was 170,000.
  - Source: http://www.wpwhitesecurity.com/wordpress-news/statistics-70-percent-wordpress-installations-vulnerable/

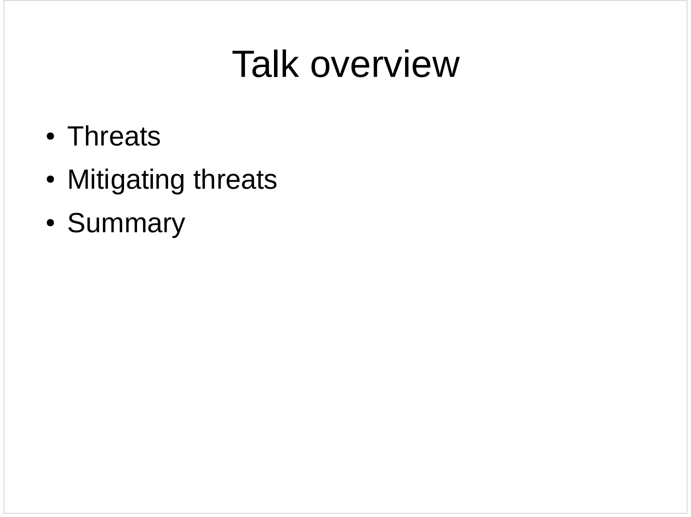
Introduction

- Again, from WP White Security, the attack vector was:
  - 41% a security vulnerability on their hosting platform
  - 29% a security issue in the WordPress Theme they were using
  - 22% a security issue in the WordPress Plugins they were using
  - 8% had a weak password.



Introduction

- YOU are a target.
- Attackers want to send spam, attack others from your site, etc.



Talk overview

- Threats
- Mitigating threats
- Summary

Threats to blogs

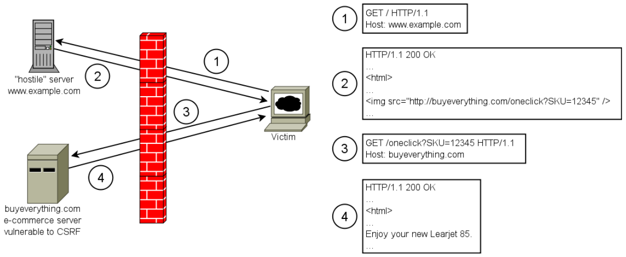
- All security starts with a threat model
  - What are you protecting
  - What are the threats against it

Threats to your readers

- Cross-site scripting (XSS)
  - Attacker uses your blog to attack your readers
  - Problem occurs when software does not produce clean output
  - i.e. it fails to encode special characters like < into `&#60;` or `&lt;`
  - Attack often targets browser vulnerabilities.
    - e.g., Microsoft's latest patches include browser fixes; there was an Apple Safari bug in May.
  - The extent of the attack is often limited by the attacker's imagination. E.g. spyware, bots, advanced persistent threats, ...

Threats to the blog

- Cross-site request forgery (CSRF)



1
```
GET / HTTP/1.1
Host: www.example.com
```

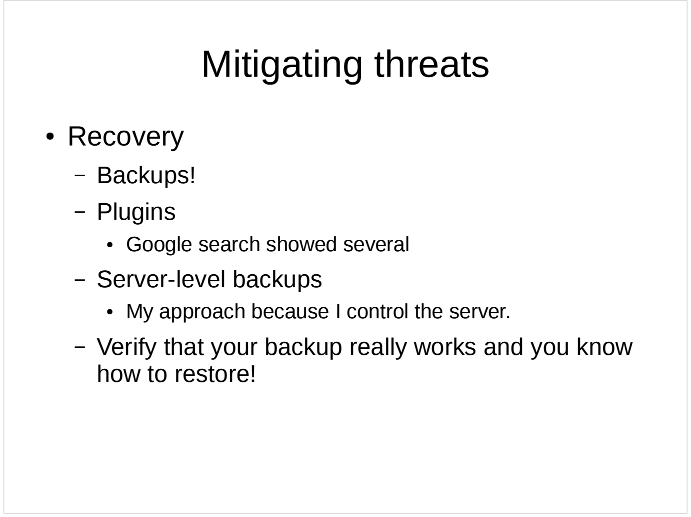
2
```
HTTP/1.1 200 OK
…
<html>
…
<img src="http://buyeverything.com/oneclick?SKU=12345" />
…
```

3
```
GET /oneclick?SKU=12345 HTTP/1.1
Host: buyeverything.com
```

4
```
HTTP/1.1 200 OK
…
<html>
…
Enjoy your new Learjet 85.
…
```

Threats to underlying operating system

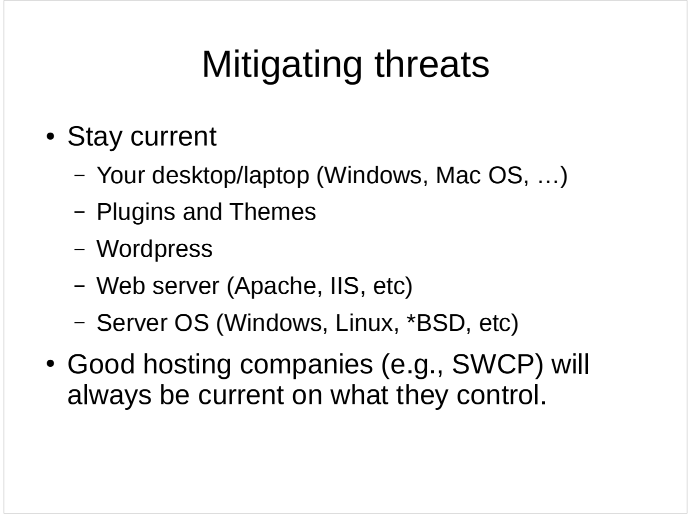
- DoS
- Run arbitrary commands (priv or not)



Mitigating threats

- Recovery
  - Backups!
  - Plugins
    - Google search showed several
  - Server-level backups
    - My approach because I control the server.
  - Verify that your backup really works and you know how to restore!

I verified my server-level backups when I wrote this slide :-)



Mitigating threats

- Stay current
  - Your desktop/laptop (Windows, Mac OS, …)
  - Plugins and Themes
  - Wordpress
  - Web server (Apache, IIS, etc)
  - Server OS (Windows, Linux, *BSD, etc)
- Good hosting companies (e.g., SWCP) will always be current on what they control.

Mitigating threats

- Only install verified software
  - Use https for downloads.
  - Only download plugins and themes from https://wordpress.org/ or from your paid vendor's web site.
  - Beware plugins not updated in a while.
  - If the software has a digital signature, verify it.

Mitigating threats

- Minimize attack surface
  - Delete plugins and themes you do not use.
    - Plugins and themes often are updated more slowly than core software.
  - Disable parts of the blog you do not use.

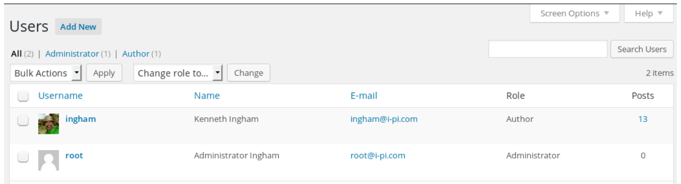
Mitigating threats

- Least privilege
  - A user has no more privileges than required for the task.
  - Wordpress user account roles:

Role	Privileges
Super admin	Administer multiple blog sites
Administrator	Control all facets of a single blog
Editor	Publish and manage posts from other users
Author	Publish and manage their own posts
Contributor	Write and mange their own posts, but cannot publish them
Subscriber	Manage their user profile

Mitigating threats

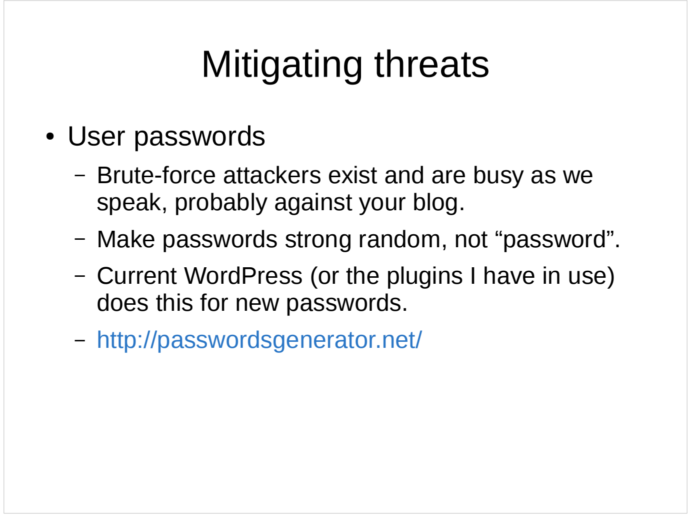
- Least privilege
  - Consider using a separate account for administration and blog writing.
  - This limits the damage an attacker can do when an account is compromised.



All (2) | Administrator (1) | Author (1)

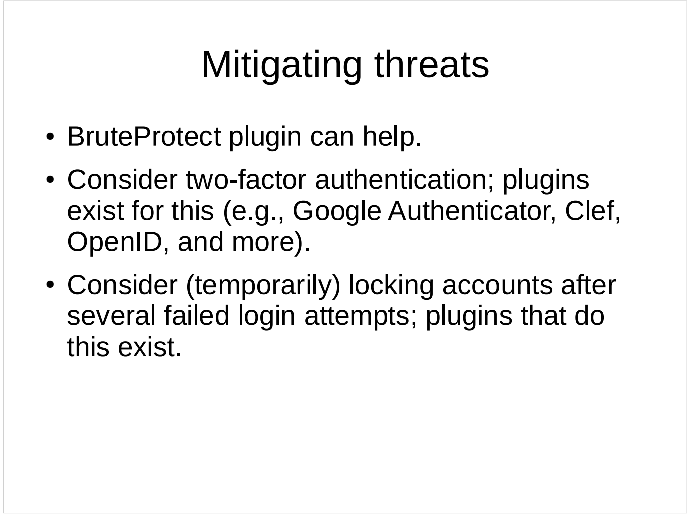
2 items

	Username	Name	E-mail	Role	Posts
□	ingham	Kenneth Ingham	ingham@i-pi.com	Author	13
□	root	Administrator Ingham	root@i-pi.com	Administrator	0



Mitigating threats

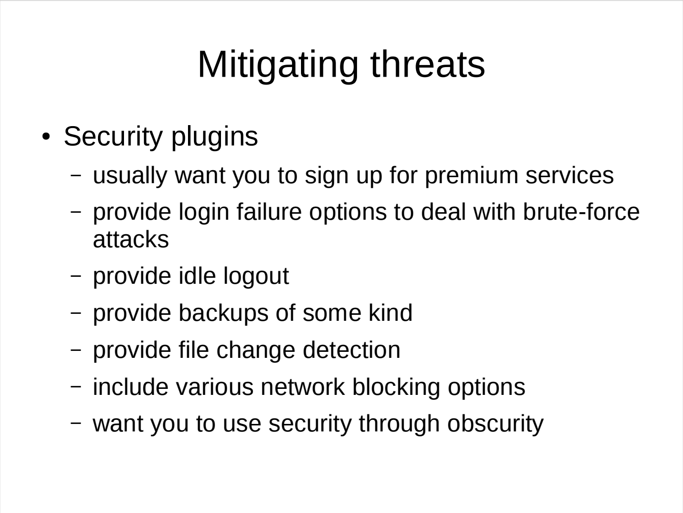
- User passwords
  - Brute-force attackers exist and are busy as we speak, probably against your blog.
  - Make passwords strong random, not “password”.
  - Current WordPress (or the plugins I have in use) does this for new passwords.
  - http://passwordsgenerator.net/



Mitigating threats

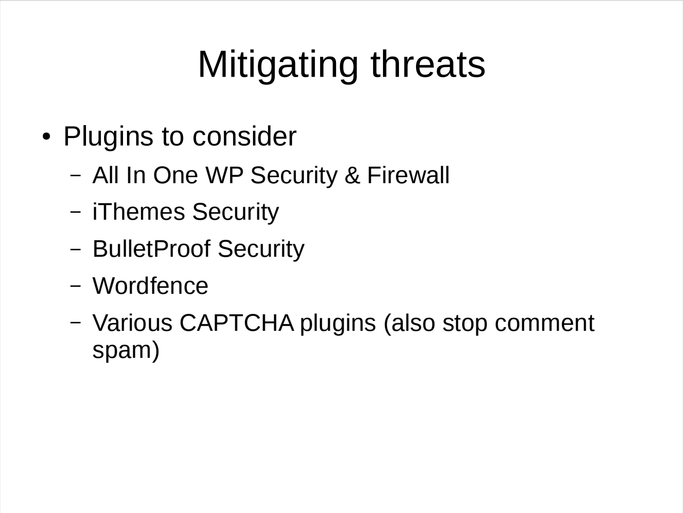
- BruteProtect plugin can help.
- Consider two-factor authentication; plugins exist for this (e.g., Google Authenticator, Clef, OpenID, and more).
- Consider (temporarily) locking accounts after several failed login attempts; plugins that do this exist.

There is a google authenticator plugin and another plugin that removes the 2FA box for users without it enabled for Google.



Mitigating threats

- Security plugins
  - usually want you to sign up for premium services
  - provide login failure options to deal with brute-force attacks
  - provide idle logout
  - provide backups of some kind
  - provide file change detection
  - include various network blocking options
  - want you to use security through obscurity



Mitigating threats

- Plugins to consider
  - All In One WP Security & Firewall
  - iThemes Security
  - BulletProof Security
  - Wordfence
  - Various CAPTCHA plugins (also stop comment spam)

All-in-one looked a little simpler and had fewer bad assumptions.

Ithemes had some good ideas and ones I considered less important. It also was unable to deal with my installation correctly.

BulletProof Security wanted to play with the files directly, something I do not allow.

Wordfence is mostly based on their paid service. It is slightly useful otherwise. It is heavily signature-based, with associated limits.

Mitigating threats

- Use all the normal “best practices for safe computing”.
- e.g., Avoid public WiFi threats.
  - Attackers set up bogus hot spots and perform man-in-the-middle attacks
  - Even non-hostile hot spots are rarely encrypted so others can eavesdrop
  - Verify HTTPS
  - **Never** click through certificate errors

Mitigating threats

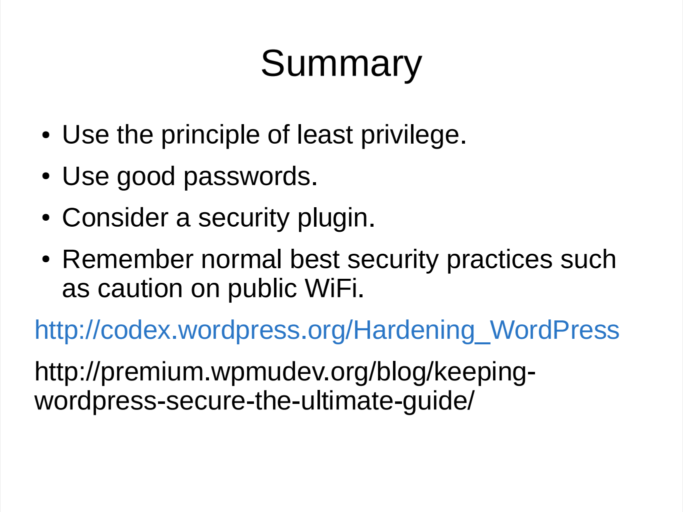
- e.g., non-encrypted communication is bad.
  - Use sftp or scp to copy files to/from server.
  - Use https whenever it is available.
- e.g., log out when you are done.

Is Wordpress secure?

- Properly-run, Wordpress does not represent a security problem.
- The key point is “properly-run”.

Summary

- Your blog faces threats to your readers, the blog itself, and the underlying OS.
- Start your mitigation strategy with a verified backup strategy.
- Next, staying current on OS, web server SW, WP core, plugins, and themes is your best defense.
- Only install verified software.
- Minimize your attack surface.

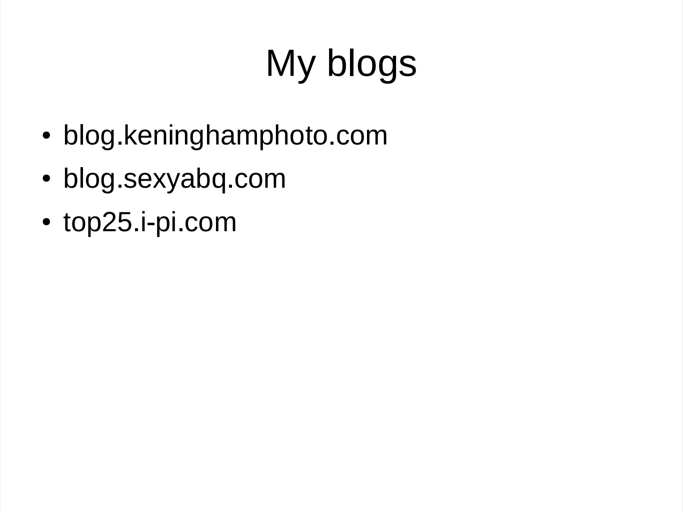


Summary

- Use the principle of least privilege.
- Use good passwords.
- Consider a security plugin.
- Remember normal best security practices such as caution on public WiFi.

http://codex.wordpress.org/Hardening_WordPress

http://premium.wpmudev.org/blog/keeping-wordpress-secure-the-ultimate-guide/



My blogs

- blog.keninghamphoto.com
- blog.sexyabq.com
- top25.i-pi.com