Securing your site

Mikko Ohtamaa

Pycon Sweden 2014


opensourcehacker.com
moo9000

Agenda

Protecting yourself

User authentication

Two-factor authentication

Third factor

Protecting the servers

Person-to-person Bitcoin exchange

Bitcoin users are high value targets

Few friends and many problem parties: hosting providers, banks, criminals, intelligence agencies

Protect yourself

Physical access

Encrypt employees computers

Encrypt phones

Two-factor authentication on email inbox

Two-factor authentication on site admin

"Cyber hygiene"

FileVault / LUKS

Display sleep

KeePassX

SSH keys (tied to your computer login)

http://opensourcehacker.com/2012/10/24/ssh-key-and-passwordless-login-basics-for-developers/

User authentication

Passwords are dead

Most successful attacks by password stealing malware

Strong password gives only limited additional protection

Throttle login attempts

CAPTCHA threshold logins per IP (leaked credentials black market)

CAPTCHA threshold per username (spearhead brute force)

recaptcha.net

Two-factor authentication

Lack of two-factor

scenario: US	0.90%
scenario: Great-Britain	0.90%
scenario: Australia	7.58%

www.schneier.com/blog/archives/2006/11/fighting_fraudu.html

TOTP - time-based

HOTP - one-time pad

SMS

USB (YubiKey)

“Calculators”

Time-Based One-Time Password Algorithm

TOTP a.k.a Google Authenticator

RFC 6238

Google apps on Android, iOS,

Other platforms and OSS implementations

HMAC-Based One-Time Password Algorithm

HOTP, RFC 4226 a.k.a. paper codes

Common in Nordic internet banking, unheard in many countries

Key: C6R1O8FJQHB **PRINT THIS ON PAPER**

1	504609	**10**	613652	**19**	984096	**28**	923915	**37**	554661
2	254567	**11**	593621	**20**	381448	**29**	848162	**38**	077193
3	834244	**12**	031369	**21**	224700	**30**	714767	**39**	052795
4	925986	**13**	102593	**22**	138068	**31**	785758	**40**	335162
5	677081	**14**	919408	**23**	744038	**32**	452522	**41**	504945
6	337361	**15**	284377	**24**	781247	**33**	889152	**42**	911086
7	755443	**16**	069350	**25**	110740	**34**	658233	**43**	740786
8	108373	**17**	312088	**26**	397198	**35**	862564	**44**	715094
9	045360	**18**	557536	**27**	058478	**36**	662422	**45**	974471
46	821321	**55**	615355	**64**	171222	**73**	451345	**82**	515858
47	873386	**56**	436935	**65**	712438	**74**	283932	**83**	047679
48	993205	**57**	844706	**66**	406619	**75**	621241	**84**	554108
49	204070	**58**	694507	**67**	445969	**76**	183450	**85**	395707
50	607447	**59**	253310	**68**	514672	**77**	365353	**86**	506355
51	873481	**60**	294116	**69**	062477	**78**	477964	**87**	168640
52	075671	**61**	076864	**70**	358581	**79**	307909	**88**	114092
53	500434	**62**	369902	**71**	249919	**80**	276411	**89**	892209
54	913334	**63**	860765	**72**	755230	**81**	659036	**90**	870758

https://github.com/LocalBitcoins/django-twofactor

http://django-two-factor-auth.readthedocs.org/

twofactorauth.org

authy.com (… you don't want to depend on a service)

Third factor

Users lose their credentials

Recycled passwords

Phishing (Google Adwords attack)

Stolen two-factor codes

Third factor parameters

Unknown web browser (identified by cookie)

The of country of IP address

The reputation of IP address (botnet, Tor, VPS)

IP address whitelist

Confirm by email or by SMS “is it really you”

Session hijacking

Tie session cookie to an IP address

Protection against cookie stealing malware

Pain for the users, especially mobile

Mad general problem

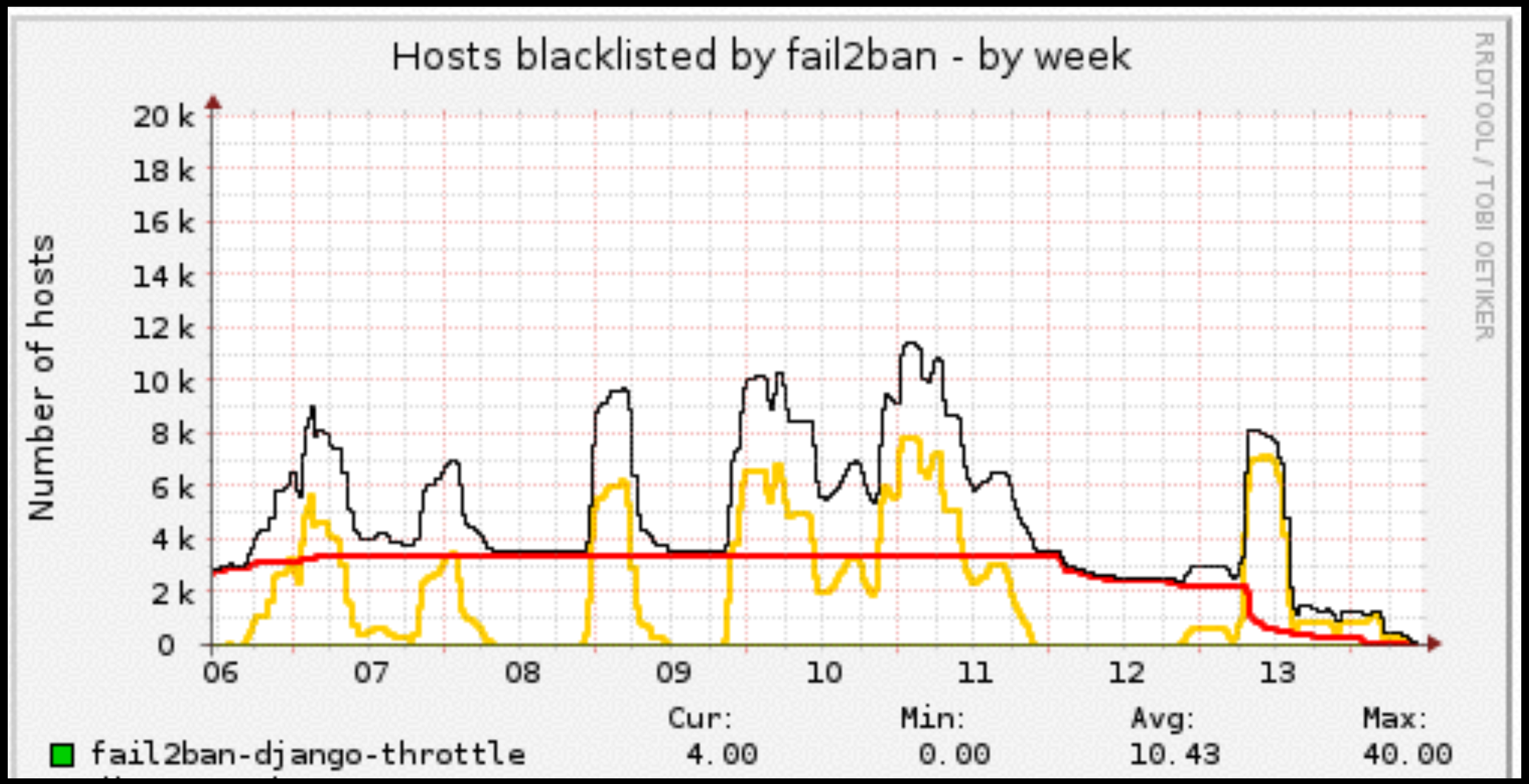
“If your local computer is compromised by malware or anything else, it is just like a mad general”

We have seen: malicious browser add-on modifying Bitcoin sites in fly, Android and iOS malware, SMS capture attacks

http://www.reddit.com/r/Bitcoin/comments/2573rw/bitcoin_is_secure_because_it_solves_the_byzantine/

Protecting your server

fail2ban



!!! Python Helsinki hangout broadcast tomorrow by Yaroslav Halchenko

Known bad IPs: projecthoneypot.org

Attack mitigation as a service: cloudflare.net

Phishing site reporting:

google.com/safebrowsing/report_phish/

mywot.com

phishtank.com

Flood attacks

Mostly harmless / reputation hit

Have throttling and banning per IP

Flood actions: password reset email, invite email, anonymous forms, user messaging

One approach: let fail2ban take care of this with custom files

Encrypted servers

Encrypt your server content - “mad hosting provider”

Encrypt backups: GPG, duplicity

Encrypt server-to-server connections: AutoSSH, VPN

Virtual machines (VPS) are always unsafe

http://blog.bitly.com/#85169217199

Django weaknesses

No POST logout

CSRF and session token recycling

Unsafe ImageField uploads

Password reset email expiration

TACK SÅ MYCKET

ALSO IN IRC!

opensourcehacker.com

Open Source Hacker

moo9000

mikko@opensourcehacker.com