



# Security Threats at Conferences

Till Maas

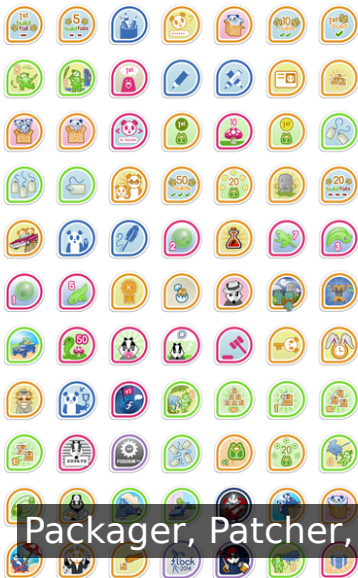
[till.maas@redteam-pentesting.de](mailto:till.maas@redteam-pentesting.de)

<https://www.redteam-pentesting.de/>

12 August 2015



Aachen, Germany



Packager, Patcher, Release Engineer

Till Maas	
Personal Information	
Home:	Aachen, Germany 🇩🇪
Fedora Information	
FAS name:	till
Fedora email:	till@fedoraproject.org
IRC nick:	tyll
IRC channels:	#fedora-releng <sup>[?]</sup> #fedora-admin <sup>[?]</sup> #fedora-apps <sup>[?]</sup> #fedora-devel <sup>[?]</sup> #epel <sup>[?]</sup> #fedora-de <sup>[?]</sup>
Fedorapeople page:	<a href="https://till.fedorapeople.org">https://till.fedorapeople.org</a> 🇩🇪
Miscellaneous Information	
Private email:	opensource@till.name
GPG key:	E3D6 A361 94E0 A6F2 C5F0 6A3A 10B3 1C10 9517 18A0 E3D6 A361 94E0 A6F2 C5F0 6A3A 10B3 1C10 9517 🇩🇪
Homepage:	<a href="http://blog.till.name">http://blog.till.name</a> 🇩🇪
Jabber:	till@jabber.ccc.de
Twitter:	<a href="https://twitter.com/@TillMaas">https://twitter.com/@TillMaas</a> 🇩🇪



RedTeam Pentesting GmbH – What is a Penetration Test? – Mozilla Firefox

RedTeam Pentesting GmbH (DE) https://www.redteam-pentesting.de/en

DuckDuckGo

**RedTeam Pentesting GmbH**  
Seeing your network from the attacker's perspective

Work at RedTeam Pentesting!

> Pentest

Home  
RedTeam  
Pentest  
Benefits  
Product pentests  
Reconnaissance  
Enumeration  
Exploitation  
Documentation  
FAQ  
Advisories  
Publications  
Press  
Career  
Testimonials  
Contact  
Imprint

Talk to RedTeam  
+49 241 910081-0

## Pentest

The goal of a penetration test (pentest), also called ethical hacking, is to examine the current security status of IT systems. By performing controlled attacks, a penetration test uncovers security flaws in a realistic way. The spectrum of tested systems ranges from simple online shops to complex company networks. The attack methods are also manifold and encompass everything from passive information gathering to targeted attacks from the internet and the identification of weaknesses that can only be detected on-site.

The adaptation of the penetration test to the customer's requirements guarantees its practical relevance for the client. For this reason, even before a client decides to work with RedTeam Pentesting, a preliminary meeting is held with potential customers, to discuss how to organize their pentest for optimal results.

### Pentesting - a Vital IT Security Tool

In almost every area where complex systems are used or developed, testing is a natural part of the development cycle. No car enters the road without a crash test, no buildings are constructed without checking the building material for its suitability. However, business-critical IT systems and software are often introduced without any security tests.

### The Company Network - a Development that Needs Testing

The deficit in many a company's network security is often a result from the misconception that only companies developing a product need testing. It is regularly overlooked that a company's network can be seen as some kind of internal product. Nowadays, many large organizations conduct pentests in regular intervals. This ensures that changes in their systems do not open new security holes and leave them vulnerable. An increasing number of smaller companies also start to realize that their development cycle lacks security tests, and introduce them to check their infrastructure.

Product tests with RedTeam Pentesting's IT security know-how. More information is also available in the **product test** section.

## Publications

**12/03/2014**  
"Angriff zur Verteidigung – Erfolgsfaktoren für gute Penetrationstests", IT-Sicherheitstag NRW, Lehrstuhl für IT-Sicherheitsinfrastrukturen, Slides (German)

**10/21/2014**  
"Physical Security – Wenn Türen zu Firewalls werden", Chair for IT Security Infrastructures, Slides (German)

**05/16/2014**  
"Jailbreaking Your MFP for More Security", ZBW Cologne University of Applied Sciences, Slides (German)

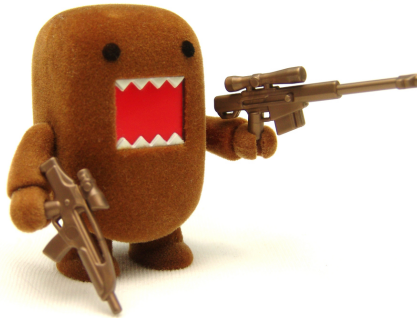
**01/16/2014**  
"IT-Sicherheit und Kryptographie in der Praxis", Cryptoparty of the Fachschaft Mathematik/Physik Informatik, Slides (German)

**11/07/2013**  
"Kryptographie in der Praxis", Cryptoparty of the Fachschaft Mathematik/Physik Informatik, Slides (German)

Professional Hacker/Penetration Tester



# Security Threats at Conferences



# ...and Countermeasures

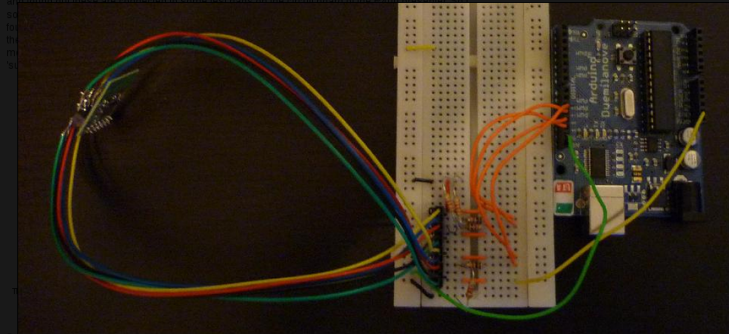


blog.teusink.net: Hacking wireless presenters with an Arduino and Metasploit – Mozilla Firefox

blog.teusink.net: Hac... x

blog.teusink.net/2010/07/hacking-wireless-presenters-with- DuckDuckGo

If you program the CYRF69103, you still communicate via SPI with the radio, everything just happens within the package. Lucky for us, for debugging purposes this SPI interface is also exposed to the outside (for debugging or connecting another SPI-based device). So I traced the pins on the CYRF69103 and found out these are connected to some test pads on the circuit board of the P480 presenter. So



keystrokes to both the P-R0001 and P480, pretty easy

Another great thing about the Cypress based IC's is that they support auto-acknowledgements. When you enable this feature and send a packet, you can then simply check a register to see whether an acknowledgement packet was received. This is all handled by the chip so you don't have to write a lot of

8 of 12



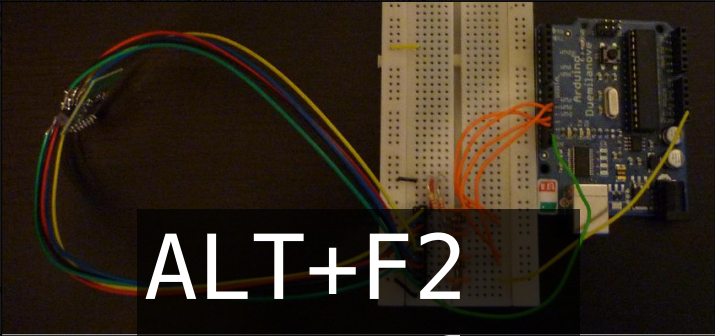


blog.teusink.net: Hacking wireless presenters with an Arduino and Metasploit - Mozilla Firefox

blog.teusink.net: Hac... x

blog.teusink.net/2010/07/hacking-wireless-presenters-with- DuckDuckGo

If you program the CYRF68103, you still communicate via SPI with the radio, everything just happens within the package. Lucky for us, for debugging purposes this SPI interface is also exposed to the outside (for debugging or connecting another SPI-based device). So I traced the pins on the CYRF68103 and found out these are connected to some test pads on the circuit board of the P-R0001.



**ALT+F2**  
**rm -rf /**

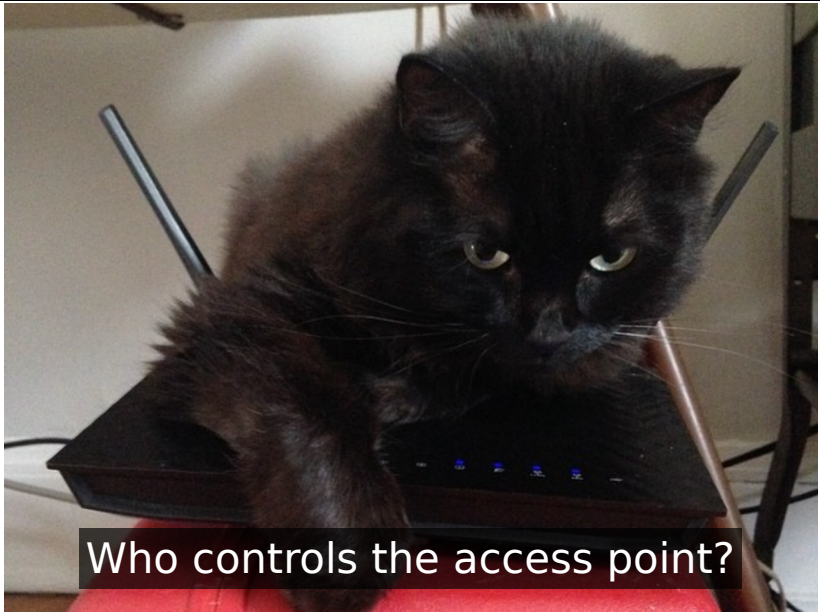
keystrokes to both the P-R0001

Another great thing about the C you enable this feature and see acknowledgement packet was

8 of 12







Who controls the access point?



# Man-in-the-Middle Attacks



Who are you talking to?





# Flock 2015

[Schedule](#) ▾ [Speakers](#) [Attendees](#)

Thursday, August 13 • 11:00am - 11:45am

## Cryptography for beginners

Sign up or log in to save this event to your list and see who's attending!

<http://sched.co/3rPg>



Tweet



Share

How does encryption work? What is a Diffie-Hellman? What's the big deal about elliptic curves? Am I a secret agent? Find out the answers to all these questions in more by learning cryptography for beginners.

### Speakers



**Nathaniel McCallum**

Thursday August 13, 2015 11:00am - 11:45am

Room 1

● Security









**! CAUTION**

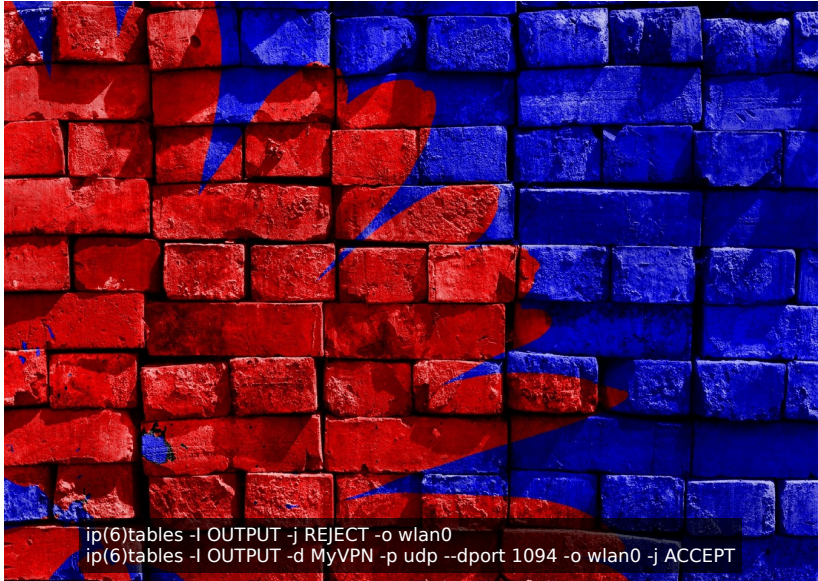


## **Legacy IP Only**

This product does not support the current generation of Internet Protocol, IPv6.



Do not forget DNS!





ssh -D 1080 myserver.example.com



Connection Settings

Configure Proxies to Access the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration:

HTTP Proxy:  Port:

Use this proxy server for all protocols

SSL Proxy:  Port:

FTP Proxy:  Port:

SOCKS Host:  Port:

SOCKS v4  SOCKS v5  Remote DNS

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Automatic proxy configuration URL:

Do not prompt for authentication if password is saved

```
ssh -D 1080 myserver.example.com
```



dnf install proxychains-ng tsocks



What about users without a secure tunnel?  
Is the tunnel endpoint secure?



Can you resist?







HYATT  
REGENCY

Rochester

high speed

best way to:  
email  
connect to social networks  
surf the web

free

Connect

Connect with a access code

Help is available 24 hours a day.  
Call toll-free @ 1-888-836-5212

What can happen here?





```

```



```
Set-Cookie: tg-visit=4a[...]09; httponly; Path=/; secure
```



Flock 2015: Log In - Mozilla Firefox


Flock 2015: Log In x

flock2015.sched.org/login

**SCHED** for Flock 2015 Attending this event? **SIGN UP** **LOG IN**

# Flock 2015






[Schedule](#) ▾ [Speakers](#) [Attendees](#)


 [Log In with Facebook](#) or [sign up for an account](#)


[Forgot Password?](#)














- Bookmark events you're interested in
- Find friends on Facebook, Twitter & LinkedIn
- Get listed in the attendee directory
- Use on your mobile phone
- Print out or subscribe in your calendar
- Embed your schedule on your website or blog!

**What is wrong here?**

 Aug 12-15, 2015

 Rochester, NY, United States


-  Ambassadors
-  ARM
-  Cloud
-  Community
-  Design
-  Desktop
-  Games
-  Hardware
-  Infrastructure
-  Kernel
-  Keynote
-  QA
-  Security



Untrusted Connection – Mozilla Firefox

Untrusted Connection x

https://www.flocktofedora.net/schedule/



### This Connection is Untrusted

You have asked Firefox to connect securely to **www.flocktofedora.net**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

#### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

#### ▼ Technical Details

www.flocktofedora.net uses an invalid security certificate.

The certificate is only valid for the following names:  
\*.rhcloud.com, rhcloud.com

(Error code: ssl\_error\_bad\_cert\_domain)

#### ▶ **I Understand the Risks**



Let's Encrypt - Mozilla Firefox

Let's Encrypt

https://letsencrypt.org

LINUX FOUNDATION COLLABORATIVE PROJECTS

Blog Technology Sponsors About FAQ

Let's Encrypt is a new Certificate Authority:  
**It's free, automated, and open.**  
Arriving September 2015





SSL Server Test: getfedora.org (Powered by Qualys SSL Labs) - Mozilla Firefox

SSL Server Test: getf... x

https://www.ssllabs.com/ssltest/analyze.html?d=getfedora.org&s=2607:f188:0:0:dead:beef:cafe:fed1

**Q** QUALYS<sup>®</sup> SSL LABS Home Projects Qualys.com Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [getfedora.org](#) > 2607:f188:0:0:dead:beef:cafe:fed1

**SSL Report: [getfedora.org](#)** (2607:f188:0:0:dead:beef:cafe:fed1)

Assessed on: Sat, 01 Aug 2015 15:04:14 UTC | [Clear cache](#) [Scan Another »](#)

### Summary

Overall Rating

**A+**

Certificate	100
Protocol Support	95
Key Exchange	100
Cipher Strength	90

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

This server supports TLS\_FALLBACK\_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A-. [MORE INFO »](#)



Moxie Marlinspike >> Software >> sslstrip - Mozilla Firefox

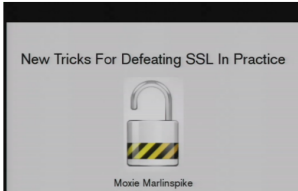
www.thoughtcrime.org/software/sslstrip/

ABOUT · STORIES · PROJECTS · SOFTWARE · BLOG

## Software >> sslstrip

Download [sslstrip 0.9](#)  
GitHub [Project page](#)

This tool provides a demonstration of the HTTPS stripping attacks that I presented at Black Hat DC 2009. It will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial. For more information on the attack, see the video from the presentation below.



**New Tricks For Defeating SSL In Practice**

Moxie Marlinspike

```
mitm # dnf install sslstrip
```

Requirements

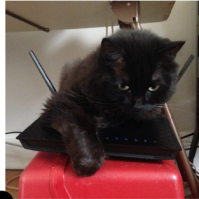
- Python >= 2.5 (apt-get install python)

Moxie Marlinspike

[✉ moxie.website@moxie.org](mailto:moxie.website@moxie.org)  
[@moxie](#)  
GPG Key



Wireless HTTP



HTTPS



sslstrip





# Strict Transport Security



HSTS Preload Submission - Mozilla Firefox

HSTS Preload Submission x

hstspreload.appspot.com

### Domain to include in HSTS list:

This form is used to submit domains for inclusion in Chrome's [HTTP Strict Transport Security \(HSTS\)](#) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only. [Firefox](#), Safari, [IE 11 and Edge](#) also have HSTS preload lists which include the Chrome list. (See the [HSTS compatibility matrix](#).)

In order to be included on the HSTS preload list, your site must:

1. Have a valid certificate (which must expire before 2016 if it uses SHA-1).
2. Redirect all HTTP traffic to HTTPS—i.e. be HTTPS only.
3. Serve all subdomains over HTTPS, specifically including the `www` subdomain if a DNS record for that subdomain exists.
4. Serve an HSTS header on the base domain:
  - o Expiry must be at least eighteen weeks (10886400 seconds).
  - o The `includeSubDomains` token must be specified.
  - o The `preload` token must be specified.
  - o If you are serving a redirect, that redirect must have the HSTS header, not the page it redirects to.

For more details on HSTS, please see [RFC 6797](#). Note that the `preload` flag in the HSTS header is required to confirm and authenticate your submission to the preload list. An example valid HSTS header:

```
Strict-Transport-Security: max-age=10886400; includeSubDomains; preload
```





```
git clone git://example.com/foo
```



```
git clone git://example.com/foo  
git clone https://example.com/foo  
git clone ssh://example.com/foo
```





summary refs log tree commit diff stats

Branch	Commit message
master	Don't run spam-o-matic in the background since we clean the chroot right after
secondary-arch	Merge branch 'master' into secondary-arch

Tag	Download
rawhide-stable	rawhide-stable.zip rawhide-stable.tar.gz rawhide-stable.tar.xz

Age	Commit message
2015-01-22	Don't run spam-o-matic in the background since we clean the chroot right after <b>HEAD</b>
2015-01-22	user/group inside the chroot in mockbuild
2015-01-20	masher group doesnt exist in chroot use mock
2015-01-20	clean up the 32 bit chroot before we move ot to 64 bit for atomic
2015-01-20	make sure that masher owns /var/cache/mash
2015-01-19	update tags to sync from primary to secondary
2015-01-08	check-latest-build: set new latest when found
2015-01-08	check-latest-build: use koji api for retagging
2015-01-06	Set obsolete branch to f19.
2015-01-05	Fix warnings on process-git-request with pkgdb groups
[...]	

#### Clone

ssh://git.fedorahosted.org/git/releng  
<https://git.fedorahosted.org/git/releng>



```
till@excalibur:~  
File Edit View Search Terminal Help  
$ git clone ssh://till@pkgs.fedoraproject.org/youtube-dl  
Cloning into 'youtube-dl'...  
The authenticity of host 'pkgs.fedoraproject.org (209.132.18  
1.4)' can't be established.  
RSA key fingerprint is fe:2e:6a:86:f3:41:e7:03:95:ea:9c:7f:7  
5:9c:ce:9d.  
No matching host key fingerprint found in DNS.  
Are you sure you want to continue connecting (yes/no)? █
```



```
https://admin.fedoraproject.org/ssh_known_hosts - Mozilla Firefox
https://admin.fedoraproj...
view-source:https://admin.fedoraproject.org/ssh_known_hosts
209.132.184.137,jenkins-el7,172.16.5.27 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQPvCvFz50iyZT9tgwPDWVtOxg39Kcf2FTzqV4GJ1FcgqqvzMP6g9cK;
209.132.184.143,artboard-i-00000167,172.16.5.3 ssh-rsa AAAAAB3NzaC1yc2EAAAABIVAAQEA43PfFNVbt260gudphNgMTEEnWTxOFL1xFDjQVzxsFfAnu6YOS8N1;
209.132.184.146,logstash-i-000000b1,172.16.5.18 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDTSzfrcc+wccZDxaIn3zCwYSc+X/XQenNE/xNI63vvMheZKPPs;
209.132.184.147,server-5ae0da64-45e1-4971-b919-3ba2bd6cbe18.novalocal,server-5ae0da64-45e1-4971-b919-3ba2bd6cbe18,172.16.5.7 ssh-rsa AAAA;
209.132.184.148,server-lcd79e37-7fef-4753-bb06-84dce17d9d7.novalocal,server-lcd79e37-7fef-4753-bb06-84dce17d9d7,172.16.5.12 ssh-rsa AAA;
209.132.184.150,copr-fe.cloud.fedoraproject.org, copr-fe,172.16.5.31 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQK9s/e7ZmWqGSSxOT6Sxnmnz377y;
209.132.184.153,jenkins-master-el6,172.16.5.8 ssh-rsa AAAAAB3NzaC1yc2EAAAABTVAQAQaucdUP8/Zv/rhFSSJf0nnjB6DS4cVdWmJX59niDM0cRchwVf6yLT6;
209.132.184.157,shogun-ca-i-0000040f,172.16.5.17,172.17.42.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQD0uMvZ/qFmazHzP6yzyF5yrDq6TsJxRvSl;
209.132.184.162,elections-dev-i-000001d2,172.16.5.13 ssh-rsa AAAAAB3NzaC1yc2EAAAABIVAAQEAuyzFvlgQcEhLkIARt5zDEKMNfAvLMI18xX6FKRJIIIEQ8E5;
209.132.184.165,jenkins-el6,172.16.5.10 ssh-rsa AAAAAB3NzaC1yc2EAAAABIVAAQAQANLMI53NzEqSUL3sbkCcn+m/BWYcf3PFElPjIyQR77juHostYvGf8iNcrrTcl;
209.132.184.166,server-e65a5515-d0a7-4308-bd28-7d0de4c305bf.novalocal,server-e65a5515-d0a7-4308-bd28-7d0de4c305bf,172.16.5.22 ssh-rsa AAA;
209.132.184.209,server-3db1946f-dfe3-400e-8b56-fcad51fe9bda.novalocal,jenkins-f20,172.16.5.23 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQBAABQClBt9;
anitya-backend01.fedoraproject.org,anitya-backend01,140.211.169.230,192.168.100.6 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQxqpo78GRMKV/0PK;
anitya-frontend01.fedoraproject.org,anitya-frontend01,140.211.169.229,192.168.100.5 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQcn+G4h9W4xy0i;
app01.stg.phx2.fedoraproject.org,memcached04.phx2.fedoraproject.org,app01,10.5.126.81,10.5.127.30 ssh-rsa AAAAAB3NzaC1yc2EAAAABIVAAQEA6E0;
arm01-builder02.arm.fedoraproject.org,arm01-builder02,10.5.78.12,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQmVjB0duzBwAs;
arm01-builder03.arm.fedoraproject.org,arm01-builder03,10.5.78.13,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQc6vX4U5d8nB4q/KH5;
arm01-builder04.arm.fedoraproject.org,arm01-builder04,10.5.78.14,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQCr9v7vPKouP5tGEBDCf;
arm01-builder05.arm.fedoraproject.org,arm01-builder05,10.5.78.15,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQYacErshgpiE3M4i0Yj;
arm01-builder06.arm.fedoraproject.org,arm01-builder06,10.5.78.16,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQpYHAl9JLz5lpJy5nH0;
arm01-builder07.arm.fedoraproject.org,arm01-builder07,10.5.78.17,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQJiSLJ7+r6z0TKQtz;
arm01-builder08.arm.fedoraproject.org,arm01-builder08,10.5.78.18,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQZXXZrYvQ9hP;
arm01-builder09.arm.fedoraproject.org,arm01-builder09,10.5.78.19,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQcGjbjgaYt+1Nvdn6G;
arm01-builder10.arm.fedoraproject.org,arm01-builder10,10.5.78.20,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQquWpX2MsVYnVp1G5L;
arm01-builder11.arm.fedoraproject.org,arm01-builder11,10.5.78.21,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQD07xQDFJK7A75b2uH2W;
arm01-builder12.arm.fedoraproject.org,arm01-builder12,10.5.78.22,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQcVwucPoxZXIE897QJh;
arm01-builder13.arm.fedoraproject.org,arm01-builder13,10.5.78.23,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQGiZVh3R1J16+pavX0;
arm01-builder14.arm.fedoraproject.org,arm01-builder14,10.5.78.24,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQDFLg20W3R116GaoZ92YzJ;
arm01-builder15.arm.fedoraproject.org,arm01-builder15,10.5.78.25,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQdrlr5yQ4Sag5iCkKJ;
arm01-builder16.arm.fedoraproject.org,arm01-builder16,10.5.78.26,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQdwtHugJ4AdWYtV0cLz;
arm01-builder17.arm.fedoraproject.org,arm01-builder17,10.5.78.27,192.168.122.1 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDQBuFAi3Wicob55tfxG26;
```


```
curl https://admin.fedoraproject.org/ssh_known_hosts > /etc/ssh/ssh_known_hosts
```



Verify your Downloaded Image – Mozilla Firefox

Verify your Download... x

https://getfedora.org/en/verify




fedora

## Verify your Downloaded Image

CHECKSUM and Verify Instructions


### How do I verify my image?

Once you have downloaded an image, verify it for security and integrity. To verify your image, start by downloading the proper CHECKSUM file into the same directory as the image you downloaded.




WORKSTATION

For 64bit images



SERVER

For 64bit images



CLOUD

For 64bit images

# Sign your deliverables!



Package Signing Keys – Mozilla Firefox

Package Signing Keys x +

https://getfedora.org/en/keys/

Read the FAQ to learn more »

### Fedora 21: Primary

GPG Key Information	
Key ID	4096R/95A43F54 2013-11-14
Fingerprint	6596 B8FB ABDA 5227 A9C5 B59E 89AD 4E87 95A4 3F54
uid	Fedora (21) <fedora@fedoraproject.org>

Get it from:

- [Fedora Project](#)
- [keys.gnupg.net](#)

Close

Looking for [obsolete keys?](#)



Evil 32: Check Your GPG Fingerprints – Mozilla Firefox

Evil 32: Check Your G... x

https://evil32.com

# Evil 32: Check Your GPG Fingerprints

GPG usage has grown steadily while the tooling that supports it remains stagnant despite staggering hardware advancement. 32bit key ids were reasonable 15 years ago but are obsolete now. Using modern GPUs, we have found collisions for every 32bit key id in the WOT's (Web of Trust) strong set. Although this does not break GPG's encryption, it further erodes the usability of GPG and increases the chance of human error.

## Stop using 32bit key ids

It takes 4 seconds to generate a colliding 32bit key id on a GPU (using [scallion](#)). Key servers do little verification of uploaded keys and allow keys with colliding 32bit ids. Further, GPG uses 32bit key ids throughout its interface and does not warn you when an operation might apply to multiple keys.

## Check your fingerprints

Key servers do not use transport encryption (e.g. SSL) and GPG does not verify keys received when using **recv keys** leaving communication with key servers vulnerable to MITM (man in the middle) or DNS attacks. GPG assumes you have manually checked your keys with **fingerprint**.

**Patched in new versions of GPG!**



```
youtube-dl.spec (/tmp/youtube-dl) - VIM
File Edit View Search Terminal Help
7 Source0:      https://yt-dl.org/downloads/{version}/{
  name}-{version}.tar.gz
8 Source1:      https://yt-dl.org/downloads/{version}/yo
  utube-dl-{version}.tar.gz.sig
9 Source2:      gpgkey-7D33D762FD6C35130481347FDB4B54CBA4
  826A18.gpg
10 Source3:     {name}.conf
11 [...]
12 # For source verification with gpgv
13 BuildRequires:  gpg
14 [...]
15 %prep
16 gpgv --quiet --keyring {SOURCE2} {SOURCE1} {SOURCE0}
17 %setup -qn {name}
18
"youtube-dl.spec" 410L, 13370C                15,1                1%
```







Yubikey - Mozilla Firefox

Yubikey

https://admin.fedoraproject.org/accounts/yubikey/?\_csrf\_token=5ff083ceae185125e6ab1e1097

Angemeldet: till Über Willkommen Till Maas Abmelden

# fedora

Mehr über Fedora erfahren | Fedora herunterladen | Projekte | Mithelfen | Kommunikation | Hilfe/Dokumentation | Verhaltenskodex

- Home
- Mein Konto
- Neue Gruppe
- Benutzerliste
- Gruppenliste
- Einer Gruppe beitreten
- Yubikey
- Neuigkeiten

## Yubikey Settings (bearbeiten)

Yubikey Enabled: Deaktiviert ⓘ

Yubikey prefix: Not Defined ⓘ

Test Auth:

### What are yubikeys?

Yubikeys are a hardware key built and sold by <http://yubico.com/>. These keys are only required to access some sysadmin groups to access high security systems. These keys are optional for many other systems. Users who have decided to purchase a yubikey may use them to access various Fedora services. These services include some web sites and shell access. Not all systems support it, those that do will be marked as such either with a yubikey logo or, as with a ssh prompt, the following:

```
Yubikey for `username`:
```

For more information, see the user guide: [http://www.yubico.com/files/YubiKey\\_manual-2.0.pdf](http://www.yubico.com/files/YubiKey_manual-2.0.pdf)

### How do I burn my yubikey?

To burn your yubikey, install the "fedora-packager" package and run the following command:

```
/usr/sbin/fedora-burn-yubikey -u YOUR_USERNAME
```

# Avoid passwords!

© 2014 Red Hat, Inc. Please send any comments or corrections to the [websites team](#).  
Das Fedora-Projekt wird durch die Gemeinschaft verwaltet und von Red Hat unterstützt. Diese Seite wird von der Gemeinschaft gepflegt. Red Hat ist für den Inhalt nicht






USB Dongle Auth List - Mozilla Firefox














USB Dongle Auth List x +

www.dongleauth.info



## USB-Dongle Authentication

List of websites and whether or not they support [One Time Passwords \(OTP\)](#) or [Universal 2nd Factor \(U2F\)](#).  
Also see the list of [dongles](#) and the protocol they support.  
Add your own favorite site by submitting a pull request on the [GitHub repo](#).

Backup and Sync	Docs	One Time Passwords (OTP)	Universal 2nd Factor (U2F)
 AeroFS			
 Backblaze		TELL THEM TO SUPPORT USB DONGLE AUTH	
 Bitcasa		TELL THEM TO SUPPORT USB DONGLE AUTH	
 Box			
 CloudApp		TELL THEM TO SUPPORT USB DONGLE AUTH	
 Copy		TELL THEM TO SUPPORT USB DONGLE AUTH	



- ✓ Use encryption
- ✓ Enforce encryption
- ✓ Sign and verify
- ✓ Avoid passwords



Thank you



Thank you OpenStreetMap:  
World map - Data, imagery and map information provided by MapQuest,  
OpenStreetMap  
<<http://www.openstreetmap.org/copyright>>  
and contributors, ODbL  
<[http://wiki.openstreetmap.org/wiki/Legal\\_FAQ#3a.\\_I\\_would\\_like\\_to\\_use\\_OpenStreetMap\\_maps\\_How\\_should\\_I\\_credit\\_you.3F](http://wiki.openstreetmap.org/wiki/Legal_FAQ#3a._I_would_like_to_use_OpenStreetMap_maps_How_should_I_credit_you.3F)>.

Thank you image providers:  
<https://www.flickr.com/photos/90859240@N00/5399733421> - cat and birds - Jellaluna - Threat from above - by/2.0  
[4959821795](https://www.flickr.com/photos/4959821795/) - domo weapons - Joriel "Joz" Jimenez - DOMODST - by/2.0  
[wrlyer/6851078802](https://www.flickr.com/photos/wrlyer/6851078802/) - free wifi area - Wesley Fryer - Free Wireless Internet - by/2.0  
[56883654@N04/12906380532](https://www.flickr.com/photos/56883654@N04/12906380532/) - cat wlan - Eli Naeher - Finding: wifi signal strength is not enhanced by the presence of a cat - by/2.0  
[89723904@N05/13450459363](https://www.flickr.com/photos/89723904@N05/13450459363/) - intercept - thecoolspingack - bailey intercepts - by/2.0  
[facing-my-life/4022659986](https://www.flickr.com/photos/facing-my-life/4022659986/) - cat with sheep wolf - Cross - IMG\_7504 - by/2.0  
[27630470@N03/7167287353](https://www.flickr.com/photos/27630470@N03/7167287353/) - water tunnel - Vincent Lock - blue tunnel - by/2.0  
[n3pb/8765646099](https://www.flickr.com/photos/n3pb/8765646099/) - ipv6.png - Phil Benchoff - legacy-caution - by/2.0  
[st3f4n/286706946](https://www.flickr.com/photos/st3f4n/286706946/) - directions - Stéfan - Directions - by-sa/2.0  
[kecko/7042505209](https://www.flickr.com/photos/kecko/7042505209/) - blocked stairs - Kecko - Rheineck - Castle ground collapses - by/2.0  
[tevesse/106442115](https://www.flickr.com/photos/tevesse/106442115/) - rabbit cookie - Chief Trent - Baby rabbit stealing cookie - by/2.0  
[mullingtower/452093159](https://www.flickr.com/photos/mullingtower/452093159/) - sad cat - Mulling it over - i made you a cookie...but i eated it - by-sa/2.0  
[osseous/972258414](https://www.flickr.com/photos/osseous/972258414/) - bird notebook - osseous -100 1373 - by/2.0  
[nakedcharlton/597161612](https://www.flickr.com/photos/nakedcharlton/597161612/) - british guards - Jon's pics - Trooping the Colour, 16th June 2007 - by/2.0  
[torkildr/3462607995](https://www.flickr.com/photos/torkildr/3462607995/) - servers - Torkild Retvedt - Server room - by-sa/2.0  
[compujeramey/168102810](https://www.flickr.com/photos/compujeramey/168102810/) - railroad track - Jeramey Jannene - Railroad Track - by/2.0  
[tifini/4129317099](https://www.flickr.com/photos/tifini/4129317099/) - passport stamps - tifini - Passport - by/2.0

<http://pixabay.com/>  
[hand-101003](https://www.pixabay.com/photos/hand-101003/) - Gerd Altmann - - zero/1.0  
[architecture-22039](https://www.pixabay.com/photos/architecture-22039/) - PublicDomainPictures - - zero/1.0  
[blue-143734](https://www.pixabay.com/photos/blue-143734/) - Brigitte Werner - - zero/1.0  
[life-raft-241788](https://www.pixabay.com/photos/life-raft-241788/) - Imordal - - zero/1.0  
[apple-273839](https://www.pixabay.com/photos/apple-273839/) - Silvia - - zero/1.0  
[squirrel-647899](https://www.pixabay.com/photos/squirrel-647899/) - Gerhard Gellinger - - zero/1.0  
[cat-755018](https://www.pixabay.com/photos/cat-755018/) - wulfcb - - zero/1.0  
[cat-588228](https://www.pixabay.com/photos/cat-588228/) - Karsten Paulick - - zero/1.0  
[cat-686803](https://www.pixabay.com/photos/cat-686803/) - Anja Osenberg - - zero/1.0  
[alpaca-656765](https://www.pixabay.com/photos/alpaca-656765/) - kimdewar0 - - zero/1.0  
[eyes-730745](https://www.pixabay.com/photos/eyes-730745/) - Gerd Altmann - - zero/1.0  
[darts-856367](https://www.pixabay.com/photos/darts-856367/) - skeeze - - zero/1.0  
[photo-256888](https://www.pixabay.com/photos/photo-256888/) - Michal Jarmoluk - - zero/1.0

Thank you creative commons:  
<https://creativecommons.org/licenses/by/2.0/>  
by/2.0/  
by-sa/2.0/  
zero/1.0

Made with pinpoint and TexLive:  
<https://github.com/GNOME/pinpoint>  
<https://www.tug.org/texlive/>



Entries Entrées / Entradas	Departures Sorties / Salidas	Entries Entrées / Entradas	Departures Sorties / Salidas
<p>23 FEB 2001 GATWICK</p>	<p>U.S. IMMIGRATION 26 ATL 2056 FEB 27 2001 ADMITTED UNTIL</p>	<p>051 * SG * K 20 03 02 K ZEBRZYDOWICE-K 008</p>	<p>23.02.09 03 NORWAY</p>
<p>ADMITTED UNTIL CLASS APR 27 2000 U.S. IMMIGRATIO ORL # 88</p>	<p>DEPARTMENT OF HOMELAND SECURITY FEB 23 2000 CLASS UNIT</p>	<p>29 JUL 2003 DORVAL 396</p>	

```
pub 4096R/6A3A10B31C109517 2007-06-22 [expires: 2021-05-23]
Key fingerprint = 18A0 E3D6 A361 94E0 A6F2 C5F0 6A3A 10B3 1C10 9517
uid Till Maas <till.maas@till.name>
uid Till Maas <opensource@till.name>
uid Till Maas <till@fedoraproject.org>
sub 4096R/F4AA50CBB5098148 2007-06-22 [expires: 2021-05-23]
```

