

How To Think About Online Security

A Guide for Activists

crane@riseup.net

What's "security"?

- Stopping an adversary from doing something that you don't want them to do

There's always an "adversary" involved. Maybe more than one.

Example: an email to a friend criticizing the government

- Does the govt. have the ability to intercept your email?
- Would they want to?
- Can they read it?
- If not, can they learn who the sender and recipients are?
- Will they follow you more closely now?

Example: storing files on a laptop

- Is the laptop kept somewhere safe?
- Do you need a password to read the files?
- Can the files be accessed remotely?
- Are there other copies of the files?
- Does anyone know you have interesting files?
- What would happen if the files were read?

Bad Security: Palin Email Hack

Mozilla Firefox

File Edit View History Bookmarks Yahoo! Tools Help

http://tunnel.com/index.php/1010110A/dcf596db65bd3f252c27d36ef92eb54ae8c2bb6920a5b2e1e24b9c149428bfc06e9be

Y! Search Web Fall TV Mail My Yahoo! News Games Travel Finance Answers Sports

TAKE THE SPECIAL K CHALLENGE FIND OUT MORE

Mail Contacts Calendar Notepad What's New? - Mobile Mail - Mail Options Go

Check Mail Compose Search Mail Search the Web

See your credit score - free

Folders [Add - Edit]

- Inbox (84)
- Drafts
- Sent
- Spam (9) [Empty]
- Trash [Empty]

My Folders [Hide]

- Emails for Arc...

Search Shortcuts

- My Photos
- My Attachments

ADVERTISEMENT

What is... MORTGAGE INSURANCE?

We nav off

Previous | Next | Back to Messages Mark as Unread | Printable View

Delete Reply Reply All Forward Spam Move... Go

HI SARAH Sunday, September 14, 2008 6:51 PM

From: "Amy McCorkell" <yoooper@mtaonline.net>

To: gov.palin@yahoo.com

Hey Sarah,
I am reading the paper, and have thoughts and prayers going your way.....don't let the negative press wear you down! Pray for me as well. I need strength to 1. keep employment, 2. not have to choose. Lately I just pray may God's will be done. I am trying to learn patience and to listen to God. I pray he gives you energy! Strength!
Love, Amy

Delete Reply Reply All Forward Spam Move... Go

Previous | Next | Back to Messages Select Message Encoding Go

Full Headers

Done

How did the hacker get in?

- Used “recover password” feature on Yahoo
- It asked him for birthday, zip code, and where Palin met her husband
- Answers to these questions from Wikipedia, US Post Office, and online biography

How was the hacker caught?

- Posted screen shots had URL starting with “ctunnel.com”



- ctunnel is an anonymous proxy, who was happy to give their logs to the FBI.
- Log had IP address of computer used for the hack.

Also...

- Hacker posted a message on 4chan.org under the name “rubico”
- this account had email “rubico10@yahoo.com”
- This email address connected to real name via YouTube profile

Both Palin and the hacker practiced *bad security*. The adversary won in both cases.

How To Think About Security

- Who is the adversary?
- What threats do they present?
- How can I protect myself from these threats?
- What will it cost me? What will it cost the adversary?

Security is mostly about *habits*.

It's something you *do*, not something you set up.

Things that can be threatened

- *Invisibility*: adversary can become suspicious of something you are doing
- *Contacts*: adversary can learn who you are talking to
- *Anonymity*: adversary can learn who you are
- *Privacy*: adversary can learn what you know
- *Operations*: adversary can stop you from acting, both online and offline

Securing your computer

If the back door is open, it doesn't matter if the front door is locked.

If your computer isn't secure, your communication security doesn't matter (much).

Needs to be impossible to control it remotely.

- Anti-virus software
- Anti-spyware software (beware key-loggers!)
- Network firewall

Physical security

- A firewall doesn't help when someone steals your computer
- Or reads your email while you're at lunch.
- Put a password on your computer!
- If the information really is important, encrypt the disk!

Use the operating system's tools, or PGP Whole Disk Encryption, or TrueCrypt

Password security

- “Phishing” is by far the most common way to get passwords.
- Don’t use short passwords, words in the dictionary, or personal data (like your birthday or pet’s name.)
- Use different passwords on different sites.
- Never share passwords between people! Get them their own.

Phishing

- A fake web site that asks for your password
- Most commonly: an email or a message that says you need to login somewhere, with a link to click on.
- *Always* read the URL before entering a password, or type it yourself.

Phishing Example

source: source:Untitled

OmniWeb Help The Omni Group Apple Mac OS X Omni Products Yahoo! spamweb SpamCop DNS DNSstuff
IronPort™ Threat Operations Center RFCs Wiki-SPF Times xword Telegraph xword Google Forced matrix BS

ebay eBay sent this message to **buriliss pierce (iroc92)**.
Your registered name is included to show this message originated from eBay. [Learn more.](#)

Question about Item -- Respond Now

eBay sent this message on behalf of an eBay member through My Messages. Responses sent using email will go to the eBay member directly and will include your email address.

Question from trlbch
[trlbch\(2377 ★ \)](#)
Positive feedback: 99.7%
Member since: Jun-14-99
Location: CT, United States
Registered on: www.ebay.com

Item: DELL Inspiron 9400 E1705 DUO 1.83 1GB 100GB GO 7800 256 (250001996470)
This message was sent while the listing was active.
trlbch is a **potential buyer**.

Hello, Did you sell the laptop or someone has put a fraudulent listing? If you are still seller tell me the buy it now price. Thank you

Respond to this question
Respond Now
Responses in My Messages will not include your email address.

Marketplace Safety Tip
Always remember to complete your transactions on eBay - it's the safer way to trade.
Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by reporting it to us. These "outside of eBay" transactions may be unsafe and are against eBay policy. [Learn more about trading safely.](#)

Thank you,
eBay

Details for item number: 250001996470
Item title: DELL Inspiron 9400 E1705 DUO 1.83 1GB 100GB GO 7800 256
Item URL: http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=250001996470&sspa_gname=ADME:B:AAQ:US:1
End date: Tuesday, Jun 27, 2006 06:57:14 PDT

Go to "http://www.signin-ebay-com-very.land.ru/eBay.html"

https://

Q: Who can read what I send on the internet?

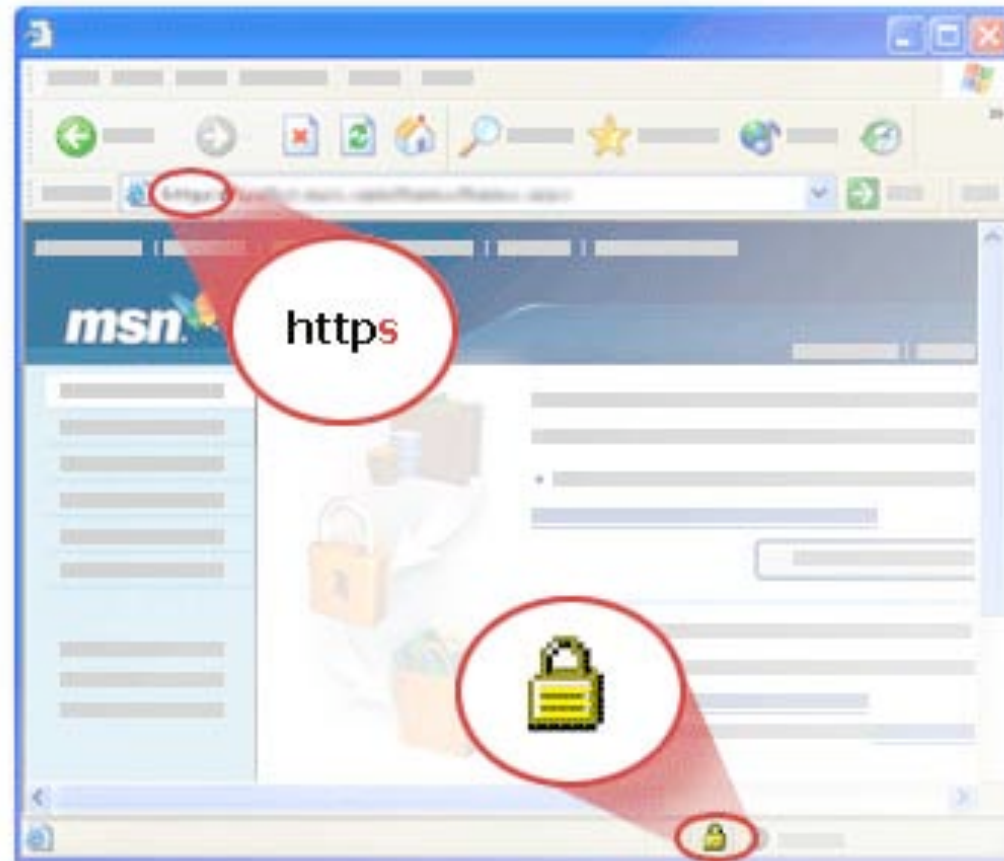
A: Everyone who runs a computer somewhere in the middle of the path that communication takes.

ISPs, Telcos, governments...

Unless: you send the data encrypted. On the web, encrypted sites start with “https”

Don't make it easy.

- Never type any sensitive information into a web page that does not start with “https”



Security is About People

- Hacking is sexy, but in reality people are the weak point.
 - ignorance, scams, “social engineering”, mistakes
 - getting lazy: sharing passwords, using insecure channels...
- Would you give up your password if...
 - they threatened to fire you?
 - they put you in jail?
 - they kidnapped your mother?

What do “they” watch?

- US, UK, Iran, Chinese governments known to have extensive electronic surveillance.
- Emails, IM, general internet traffic
- Facebook, Google, Yahoo, etc. all service *millions* of law-enforcement requests per year.
- Phones don't need to be “tapped”. It's all done through the network now.
- Basically, you have to assume that all communications are monitored.

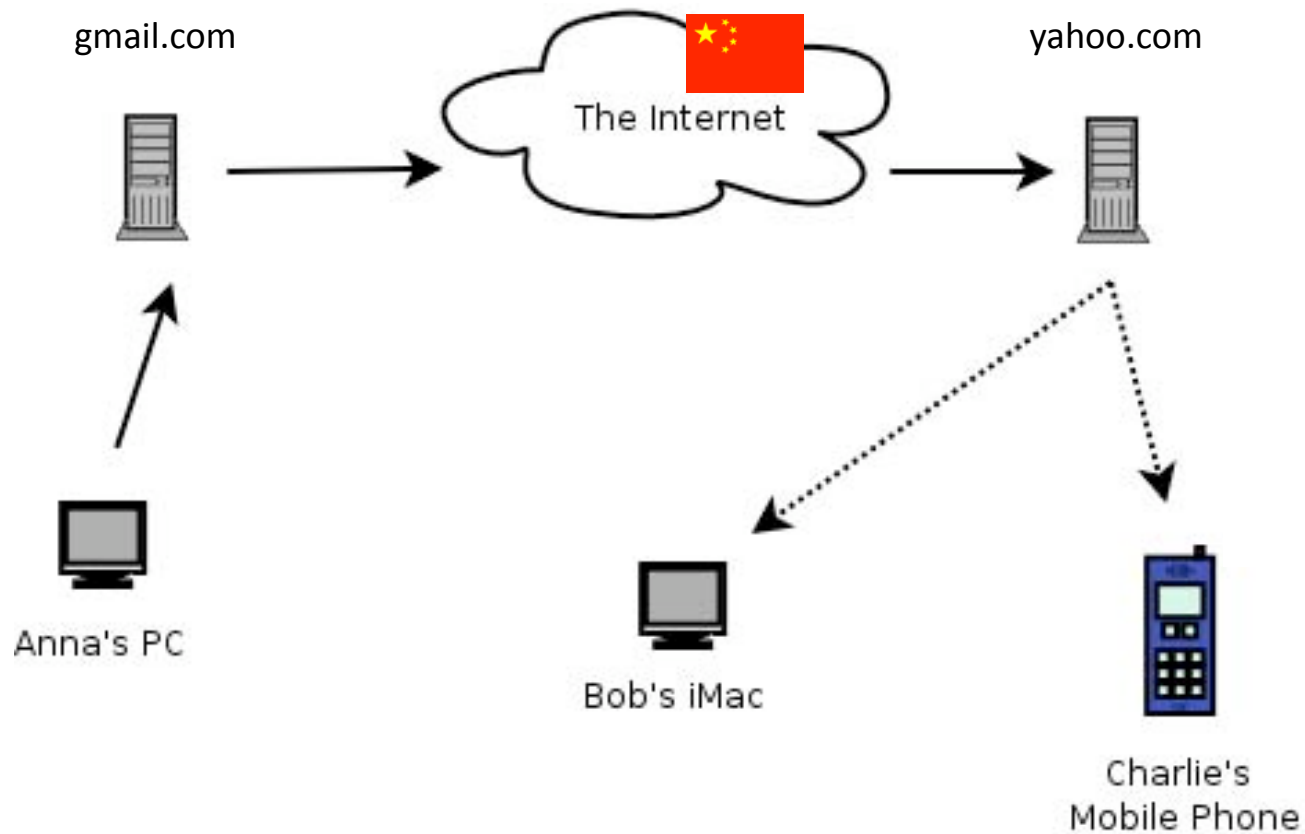
What else can “they” watch?

- Credit cards, banking transactions
- Security cameras
- Student cards, smart cards, any time you use any card...
- National governments can ask for any of this data.
- Will governments cooperate on international cases? Maybe.

Securing web email

- Gmail always uses https now
- So, the communication from your computer to Google's computer is secure.
- But then Google sends the email to the recipient's server without encryption!
- Think: where does this message go? Where are the computers physically located?

Where the Email goes



What if we both use Gmail?

- Better!
- Now the email is never sent unencrypted.
- But Google can still read it...

When does Google read emails? When the US government tells them to. Millions of requests per year.

Will Google tell other governments?

Maybe. Yahoo has.

Keeping email private, really

- You need to use something called PGP (“pretty good privacy”) to encrypt messages.
- A bit tricky. For Firefox, a tool called FireGPG makes this easier.
- If the email is encrypted properly, no one but the receiver can read it, even if it’s intercepted.
- Tutorial here:
<http://www.irongeek.com/i.php?page=videos/using-GPG-PGP-FireGPG-to-encrypt-and-sign-email-from-gmail>

The Internet is More than The Web

There are lots of ways to communicate that do not involve the web:

- Apps on your phone
- instant messaging programs
- Email through Outlook, Thunderbird, etc.
- Skype
- Twitter clients
- etc.

https won't help for these, because it's *only for web pages*.

Skype

- Skype uses strong encryption and is generally considered safe.
- Skype company (EU) knows who you're talking to, but not what you say. Will they tell?

BUT

Do *not* use Chinese TOM-Skype or clone!

Intentionally insecure! Watches for keywords and sends data to Chinese govt!

Simple secure Communication: Instant Messenger plus OTR

- OTR means “off the record.” It’s a plug-in for instant messenger programs.
- Easy!
- Just use your normal IM account, and access it from a program which supports OTR

All OS’s: use “Pidgin” plus the OTR plugin

Mac: use “Adium”

“Mostly secure” is “not secure” (like using condoms)

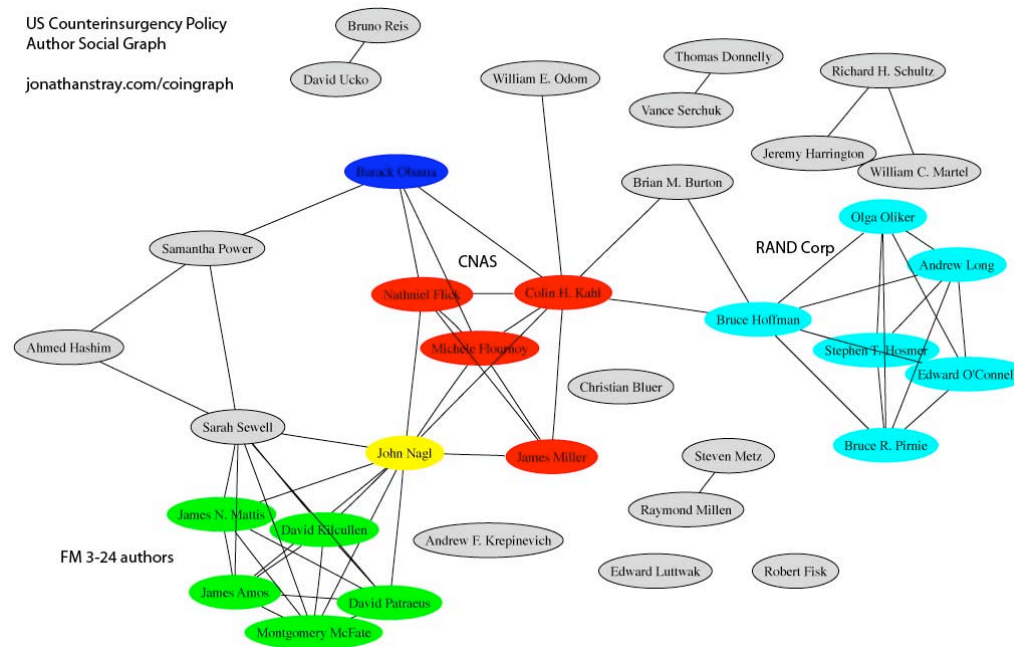
- If you need secure communications, set up IM + OTR right now.
- Communications that are “sometimes secure” are worse than useless.
- That one unencrypted message can cause problems in many different ways.
- It only takes one leak to ruin *invisibility* or *anonymity*.
- Don't be lazy.

Important!

Encryption preserves *privacy*, but not *anonymity*.

They can't read it, but they know who I'm talking to.

- Encrypted communications (like IM+OTR) protect *privacy*, but not *invisibility* or *anonymity*.



- Using encryption may be suspicious.
- They know who you are and who your friends are, and when you talked to them.

Anonymity

- Every computer on the internet has a unique number, called the “IP address”
- IP means “internet protocol.” This is how your data “knows” how to get to you.
- Most servers log the IP address of everyone who uses them.
- Your ISP sells you the IP address, so it knows who you are.

Hiding your IP Address

- Can use an “anonymous proxy”



- But does the proxy keep logs? Who can read them?

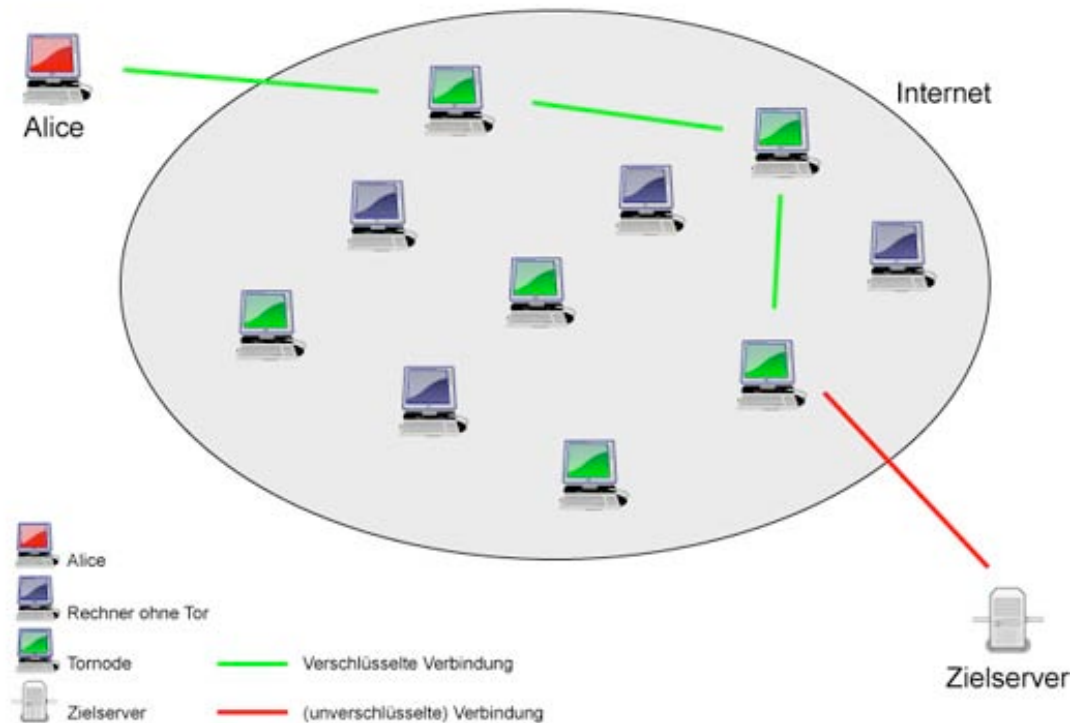
Trusting a proxy

- Anyone running a server has to give their logs to law enforcement in their jurisdiction
- E.g. a server in Canada must report to the Canadian government.
- Is this a problem? Maybe.
- What if the proxy is hacked by the adversary?
- What if the proxy is actually *run* by the adversary?

Onion Routing

- Use multiple proxies.
- No single proxy knows both the IP address of both ends of the connection

Verbindung via Tor



TOR: The Onion Router

- torproject.org
- International project to build an anonymity tool.
- The best anonymity you can currently get.
- Also jumps over firewalls very reliably!
- Slow... the network is not large.
- You can help! Run a Tor node!



Things that break anonymity

- Don't post your name, city, email, etc.!
- Don't log in to your regular email, Facebook, etc. over an anonymous connection!
- Timing attack: if you're always using Tor when a new post appears on an anonymous blog, they can tell it's you.
- Used time-delayed posting feature to avoid this.
- Anonymity is hard! If you need it, study it.

Phones

- The location of every phone is continuously logged by the telco, to within a few meters.
- Changing SIM cards won't make you anonymous, because the phone has an IMEI number.
- Text messages are logged.
- Call destination and (sometimes) audio are logged.
- Phones are *very* insecure!

Beware hidden info in documents!

- When you save a Word or PDF file, it includes your user name and other identifying information.
- This is called “metadata” and will give you away!
- Use a plain text editor to avoid this (Notepad, TextEdit)
- Or “sanitize” the document before releasing. See NSA procedures:
http://www.nsa.gov/ia/_files/support/I733-028R-2008.pdf

Avoiding Suspicion

- Decide carefully which activities are public and which are private. Speak out deliberately, not randomly.
- If you only have encrypted communications with certain people, the adversary knows exactly who you are working with!
- Use encryption whenever possible for your *regular* traffic.

Summary

How to think about security

- What are you trying to accomplish, who is trying to stop you, and how can they do it?
- Design your security to protect against *specific threats*.
- Things that can be threatened: *invisibility, contacts, anonymity, privacy, operations*.
- Security is something you *do*.
- It changes fast! Keep learning!

What To Do

- Make a security plan!
- Secure your computers: anti-virus, anti-spyware, firewalls
- Secure your computers physically: locks, passwords, disk encryption
- Use strong passwords. Don't share them between people or accounts.
- Use secure communications.
- Sanitize released documents!
- Keep learning!

Private communications

The simplest method I know for *privacy*:

- Use instant messenger plus OTR (*always!*)
- *Never* IM from your phone!

Communication between two users @gmail is second best way – but it keeps logs, and depends on Google and US govt being on your side.

Anonymous communications

If you need *anonymity* as well as *privacy*:

- Sign up for new IM accounts anonymously – don't give your email or re-use a user name.
- Set your IM client to route through TOR
- *Always* use TOR. The one time you don't, the adversary gets your IM handle and knows who you talk to.

Anonymous email addresses

- gmail.com now requires a phone number, so not anonymous.
- riseup.net is best, but you will need to be invited by someone who already has an account.
- hushmail.com is free and very good. Can send encrypted messages to people without encryption software.

Don't ever log into your anonymous email account without Tor! Otherwise anyone watching your connection will know it's you!

I haven't talked about...

- Securing your web server.
- Denial-of-service attacks: how to keep your site up (assuming the government can't just order you to stop.)
- Smuggling data.
- Operational security: who do you trust in the "real" world? Who knows your plans? Who gets passwords?

There are many different types of security.

Keep learning!

NGO security guide (read it!) Detailed tutorials on every tool mentioned here:

<http://security.ngoinabox.org/>

Anonymous blogging with Wordpress and TOR”

<http://advocacy.globalvoicesonline.org/projects/guide/>

How to get around the Great Firewall:

<http://www.randomwire.com/how-to-bypass-the-great-firewall-of-china/>