

fundamental rights

and makes free speech risky. But we're far from helpless

to do something about it.

EmailSelfDefense.fsf.org

Free Technology Workshop

Secure Browsing and Email Bulk surveillance violates our

Web Browsing with HTTPS Secure Email with OpenPGP

Organised by Steven Gordon Room RS309 9am - 12noon Friday 27 June 2014 http://ict.siit.tu.ac.th/moodle/

Adresses

- Local copies of software
 - http://ict.siit.tu.ac.th/software/
- Presentation slides and videos
 - http://ict.siit.tu.ac.th/moodle/
- Local address for ICT
 - ict.siit.tu.ac.th (from anywhere)
 - 10.10.6.11 (from inside SIIT)

SSH Access to ICT

- Use PuTTY (Windows) or ssh (OSX, Linux)
 - Address: ict.siit.tu.ac.th
 - Username: u5412345678
 - Password: supplied to you
- Once logged in you can:
 - Change password: passwd
 - Exit: exit

SSH

SSH and Tunnelling

- ict.siit.tu.ac.th
 - username: u5412345678
 - (Replace with your student ID)
 - Password has been provided to you
- Dynamic forwarding on command line, Linux/OSX:
 - ssh -l u5412345678 -N -D 6666 ict.siit.tu.ac.th
- In browser proxy settings:
 - SOCKS host: localhost
 - Port: 6666

SSH on Windows with PuTTY

- PuTTY Configuration:
- Connection -> SSH -> Tunnels
 - Source Port: 6666
 - Destination: ict.siit.tu.ac.th
 - Select "Dynamic"

Example SOCKS Proxy in Firefox



Firefox Plugins

Firefox (and Chrome) Plugins

- HTTPS Everywhere
 - https://www.eff.org/https-everywhere
- Privacy: AdBlock Plus, Ghostery
- Safety: NoScript
- Proxy: FoxyProxy, Hola Unblocker
- Passwords: LastPass, KeeFox (KeePass)
- And many more

Free Software Foundation: Email Self Defense Guide to using encrypted email with GnuPG, Engimail and Thunderbird http://emailselfdefense.fsf.org/



Secure Email with PGP

Steps

- Install Thunderbird Email Client
 - Setup an account, e.g. gmail, hotmail or siit
- (Windows only) Install GPG4WIN
- Install Engimail Add-on in Thunderbird
- In Thunderbird:
 - Make your keys
 - Distribute your keys
 - Send signed/encrypted emails

Install Thunderbird



(Windows Only) Install GPG4Win



Index of /software/windows



Add an Account



Install Enigmail Add-on



OpenPGP Setup Wizard Sign by default: No

Steve@silt.tuta OpenPGP Setup Wizard □	- 🖋 Write	Chat Address Book Tag Tag Quick Filter Search <ctrl+k></ctrl+k>	م) =
Inbox Signing Date Draft (3) Digitally Sign Your Outgoing Emails Date 1:27 AM Digitally Sign Your Outgoing Emails 11:27 AM Ii Archives Ii allows people to be sure that an email is really from you. It's good security practice to sign all outgoing email. 11:33 AM Ii aasXN a traines Ii allows people to be sure that an email is really from you. It's good security practice to sign all outgoing email. 11:39 AM Ii Advisees To verify your signed email, people need an OpenPGP-aware mail program. If they don't have an OpenPGP-aware mail program. If they don't have an OpenPGP-operator as an attachment or as text around the email message. This might annoy some people. You need to choose if you want to sign all outgoing email, or if you want to avoid sending signed email to some people. 243 PM Chats Do you want to sign all your outgoing email by default? Yee, I want to sign all of my email ITS322 Do you want to sign all of my email No, I want to create per-recipient rules for emails that need to be signed ITS323 ITS332 ITS323 ITS333 ITS333 NRU MRU Personal	it.tu.ac)penPGP Setup Wizard	hift+K>	,
Drafts (3) Digitally Sign Your Outgoing Emails Date Sent OpenPGP allows you to digitally sign your emails. This is like the electronic version of signing a Actives 11:27 AM Junk a letter, and it allows people to be sure that an email is really from you. It's good security practice to sign all outgoing email. 11:39 AM Trash aasNN To verify your signed email, people note a rouge of your email, both the signature will be displayed as an attachment or as text around the email message. This might annoy some people. You want to choose if you want to sign all outgoing email, or if you want to avoid sending signed email to some people. 243 PM Contacts Do you want to sign all outgoing email by default? 243 PM Cottacts Do you want to sign all oury outgoing email by default? 326 PM Cities No, I want to create per-recipient rules for emails that need to be signed 749 PM ITS323 ITS324 No, I want to create per-recipient rules for emails that need to be signed 740 PM ITS325 ITS324 No, I want to create per-recipient rules for emails that need to be signed 740 PM ITS325 Personal Cancel	Sign	ing		
Sent OpenPGP allows you to digitally sign your emails. This is like the electronic version of signing a letter, and it allows people to be sure that an email is really from you. It's good security practice to sign all outgoing email. 11:33 AM Image: Trash asolvin Advises To verify your signed email, people need an OpenPGP-aware mail program. If they don't have an OpenPGP-aware mail program they will be able to read your remail, but the signature will be displayed as an attachment or as text around the email message. This might annoy some people. You need to choose if you want to sign all outgoing email, or if you want to avoid sending signed email to some people. 243 PM Contacts CSS322 Do you want to sign all outgoing email, or if you want to avoid sending signed email to some people. 243 PM CSS322 Do you want to sign all our outgoing email by default? O yes, I want to create per-recipient rules for emails that need to be signed 249 PM ITF32 ITF333 ITF3332 ITF333 ITF333 ITF333 ITF333 ITF313 ANNI NRU Sack Net> Personal Cancel	3) Digi	tally Sign Your Outgoing Emails	Date	^
Archives Open-0-3 allows you to alloging aging your emails. In its line the electronic Version or signing a letter, and it allows people to be sure that an email is really from you. It's good security practice to sign all outgoing email. 11:33 AM Junk Trash To verify your signed email, people noed an OpenPGP-aware mail program. If they don't have an OpenPOP-aware mail program they don't don'		O DCD II I I I I I I I I I I I I I I I I	11:27 AM	
Junk practice to sign all outgoing email. 11:39 AM @ Trash aasSVN To verify your signed email, people need an OpenPGP-aware mail program. If they don't have an OpenPGP-aware mail program they will be able to read your email, but the signature will be displayed as an attachment or as test around the email message. This might annoy some people. You need to choose if you want to sign all outgoing email, or if you want to avoid 11:8 PM 2:33 PM Contacts Seming signed email to some people. 2:43 PM Costacts Do you want to sign all your outgoing email by default? 2:49 PM Costacts O you want to sign all your outgoing email by default? 2:6 PM ITFS ITFS No, I want to create per-recipient rules for emails that need to be signed 1:1:32 AM ITS322 ITS32 ITS32 ITS32 ITS323 ITS32 ITS33 ITS32 Personal Cancel	s	a letter, and it allows people to be sure that an email is really from you. It's good security	11:33 AM	
© Trash aasXVN Advises Chats Contacts Co		practice to sign all outgoing email.	11:39 AM	
aaSVN aaSVN aaSVN Advises Chats Contacts Chats Contacts Contacts Contacts Chats Contacts Cont		To varify your signed entril groups and an OpenDGD super mail sectors. If they don't have	11:48 AM	
Advises be displayed as an attachment or as test around the email message. This might annoy some people. 243 PM Chats people. You need to choose if you want to sign all outgoing email, or if you want to avoid sending signed email to some people. 243 PM CS322 Do you want to sign all your outgoing email by default? Yes, I want to sign all or my email Enalied Contact Yes, I want to sign all or my email It is a signed email to create per-recipient rules for emails that need to be signed IFS2 ITS22 ITS323 ITS325 ITS324 ITS325 ITS325 ITS32 ITS413 AIST NRU <gack neet=""> Cancel</gack>		an OpenPGP-aware mail program they will be able to read your email, but the signature will	1:18 PM	
Chats people. You need to choose if you want to sign all outgoing email, or if you want to avoid 249 PM Contacts Sending signed email to some people. 326 PM CS3322 Do you want to sign all your outgoing email by default? 326 PM Enquiries Yes, I want to sign all your outgoing email by default? Yes, I want to sign all of my email IPS ITS32 No, I want to create per-recipient rules for emails that need to be signed ITS323 ITS323 ITS323 ITS323 ITS323 ITS355 ITS413 AKST NRU RRU Keet> Cancel	s	be displayed as an attachment or as text around the email message. This might annoy some	2:43 PM	
Contacts 3:26 PM Contacts 3:26 PM CS322 Do you want to sign all your outgoing email by default? Enquiries Ves, I want to sign all of my email Enquiries No, I want to create per-recipient rules for emails that need to be signed IFVE ITS323 ITS323 ITS323 ITS323 ITS323 ITS323 Ves, I want to create per-recipient rules for emails that need to be signed ITS323 Ves, I want to create per-recipient rules for emails that need to be signed ITS323 Ves, I want to create per-recipient rules for emails that need to be signed ITS323 Ves, I want to create per-recipient rules for emails that need to be signed ITS325 Ves, I want to create per-recipient rules for emails that need to be signed ITS325 Ves, I want to create per-recipient rules for emails that need to be signed ITS325 Ves, I want to create per-recipient rules for emails that need to be signed ITS325 Ves, I want to create per-recipient rules for emails that need to be signed ITS325 Ves, I want to create per-recipient rules for emails that need to be signed ITS325 Ves, I want to create per-recipient rules for emails that need to be signed INRU Vestor Method Personal Cancel		people. You need to choose if you want to sign all outgoing email, or if you want to avoid	2:49 PM	
CSS322 Do you want to sign all your outgoing email by default? Enquires Yes, I want to sign all of my email ICTES No, I want to create per-recipient rules for emails that need to be signed ITS23 ITS323 ITS323 ITS335 ITS413 AIST NRU < gack Next> Cancel	3	sending signed email to some people.	3:26 PM	
Emailed Conta Enquiries ICTES IPS IFFE ITS323 ITS332 ITS335 ITS413 ARST NRU Personal Cov want to sign all of my email O Ve, I want to sign all of my email O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I want to create per-recipient rules for emails that need to be signed O Ve, I wan		Do you want to sign all your outgoing email by default?		
Enquiries Tex, treats to sign an of my emain ICTES No, Twant to create per-recipient rules for emails that need to be signed ITS ITS ITS ITS ITS ITS ITS ITS	Contac	Ver Turant to sign all of mulemail		
ICTES INo. I want to create per-recipient rules for emails that need to be signed IPS ITS22 ITS325 ITS413 AIST NRU Personal	15			
IPS ITFE ITS323 ITS324 ITS325 ITS413 JAST NRU Personal		No, I want to create per-recipient rules for emails that need to be signed		
ITPE ITS33 ITS332 ITS335 ITS413 JAIST NRU Personal				
ITS323 ITS325 ITS335 ITS413 JAIST NRU Personal				
ITS332 ITS335 ITS413 JAIST NRU Personal				
ITS335 ITS413 JAIST NRU Personal				
ITS413 JAST NRU Personal				
AIST NRU < Back Next > Cancel				
RU Personal Cancel				
Personal Cancel				
	a la	< Back Mext > Cancel		
References	ces			

Exchange Keys

- Upload to Key Server
 - Unfortunately SIIT blocks the port used for upload
- Email Public Key to Friends
 - Manually confirm that correct key
 - ID or Fingerprint

OpenPGP Setup Wizard Generate your keypair

