Athens CryptoParty #0

Using SSL/TLS for your
Internet communications

Athens CryptoParty #0

Before you install ANY downloaded software you MUST ALWAYS check it's signature file.

https://en.wikipedia.org/wiki/Comparison_of_file_verification_software

- Windows (GUI):
  - ExactFile: http://www.exactfile.com/downloads/
    Freeware NOT Open Source :(
- Linux/OS X (command line)
  - md5sum, sha1sum, md5deep, etc

Verify Signatures file (*):

- md5sum -c signature_file.txt
- sha1sum -c signature_file.asc

Please download Wireshark for this workshop

a) Download:

- https://www.wireshark.org/download.html
- https://www.wireshark.org/download/SIGNATURES-1.8.3.txt

b) Check signatures :

- gpg –verify SIGNATURES-1.8.3.txt (very important step!)
- sha1sum -c SIGNATURES-1.8.3.txt
- Look for something like: Wireshark-win64-1.8.3.exe: OK

c) Install!

- Windows: Click-click install as Administrator
- Linux: apt-get install wireshark

Athens CryptoParty #0

Why all the fuss ? Isn't Internet secure enough ?

- What can someone who's sniffing the network see?
  - **Who** talks to **whom** ?
  - **What** do they say ?
  - **Why** does this user visit a certain site ?
  - **What** are the **contents** of a user's files **stored** on a server (e.g. e-mails) ?
- Would you like someone **CONSTANTLY** over your shoulder looking what you are doing at your computer ?
- Each user has a different **threat model**!
  - What do **YOU** care/need to protect ?

Athens CryptoParty #0

I am annoyed/worried/afraid that “bad guys”/LEA might...

- ...know to whom I send emails
- ...read my emails as I send/receive them
- ...steal my passwords as I send/receive them
- ...know which sites I visit [IP → (Tel # → Person's address → knock knock!)]
- ...know what I read/post on these sites
- ...find info about my political/activism affiliations
- ...find about my online persona
- ...find what my hard disk contains
- ...steal my laptop
- ...force ISP/Google/Facebook/Dropbox to send them my data
- ...break into my house
- ...get my laptop, fill it with malware, leave it back and spy on me forever
- ...kidnap me

Athens CryptoParty #0

- What can we hide ? And from whom ?

  https://www.eff.org/pages/tor-and-https

- Using SSL/TLS
  - ***Can*** *hide (encrypt)* **what** we say to others from "bad guys"/LEA snooping the network/internet
  - ***Can't*** *hide* **who** the source/destination is
  - ***Can't*** *protect* you from the **destination's sysadmin**!

Athens CryptoParty #0

Link Layer (cable) → Internet Layer (IP) →

Transport Layer (tcp) → Application Layer (http/imap)

- SSL: Secure Sockets Layer (old)
- **TLS**: Transport Layer Security (cur vers → 1.2)
- Encryption at the **Application layer** for use by the Transport Layer
- **Key exchange** using Asymmetric/Public key Crypto
- **Confidentiality** using Symmetric key Crypto
- **Integrity** using MAC (Message Authentication Codes)

Check your connections with Wireshark (5')

- Start wireshark as root/Admin
- Choose Interface
- Start capturing
- Play with filters
  - http
  - dns or jabber
  - tcp.port==110 and ip.addr==your.mail.srv.IP
- **Demo**: Pick an “HTTP 200 OK” reply
  - Look at “Uncompressed Entity Body” at the bottom
  - Surprise!

Check your connections with Wireshark (5')

- Go to http://google.com and search for something
  - If it's over HTTP then **anyone** on the network path from you to Google can see what you're searching for!

- Login to your webmail
- Look at the data you send and at the replies you get
  - Add proper filters so you won't get flooded with packets
- Can you read data through wireshark ?
  - Yes → So can others!
  - No → **Maybe** others can't!

Now, I check your connections :D (5')

- I'll sniff your connections at the local router, just like any “bad guy” or LEA can do.

- **Demo**!

  ssh -f root@ROUTER.IP "/usr/sbin/tcpdump -Uw - -s0 -ni INTERFACE not port 22" | wireshark -k -i -

- So...do you mind if I have access to **EVERYTHING** you read and write on the web ?

HTTPS-Everywhere

- Why?
  - Many sites support HTTPS but neither we, nor our browsers, know about it.
  - Very few people try https:// instead of http:// by default.
- Created/Supported by EFF
  - Whitelists HTTPS enabled websites
  - Download/Install HTTPS-Everywhere for **Firefox** and **Chrome** ONLY:

    https://www.eff.org/https-everywhere
- **Demo**
  - visit google.com and look at wireshark
  - It's no longer over HTTP but over HTTPS
  - Your search queries are encrypted!

HTTPS-Everywhere for Greek websites ?

- An initial list by yours trully
- Extremely few Greek websites support HTTPS! Help is needed to add more sites to the list!
- Greek rules are getting integrated upstream at version 4.X
- Clone/Add rules/Submit Pull Request!
  - https://github.com/kargig/https-everywhere-greek-rules
- You don't know how to use git ? No problem, add an issue:
  - https://github.com/kargig/https-everywhere-greek-rules/issues?state=open

Enable Mandatory HTTPS for certain sites

Facebook → Account Settings → Security → "Browse Facebook on a secure connection (https) when possible”

Gmail → Settings → General → Browser connection: “always use https”

Twitter → Always on Since 02/2012

Secure Login Form Submission (Firefox)

- A visual addon to help you know when you're submitting personal data over HTTP or over HTTPS
- Download GreaseMonkey addon
  - https://addons.mozilla.org/en-US/firefox/addon/greasemonkey/
- Add GreaseMonkey script “is_login_safe” by Aggelos Orfanakos
  - https://gist.github.com/310025

How to get SSL/TLS Server Certificates

- Greek Academia → **PKI GRNET** https://pki.grnet.gr/
  - Cooperation of **GRNET** with **Terena** and **Comodo** to provide **FREE** server and personal certificates for Academic institutions.
- Non-academic → **StartSSL** https://www.startssl.com/
  - Free Class-1 certificates
  - Valid for 1-year but with unlimited renewals
- **Comodo** 90-day trial (but why??)
  - https://www.instantssl.com/ssl-certificate-products/free-ssl-certificate.html
- Provide secure services to your clients **TODAY** for **FREE**!

HSTS → HTTP Strict Transport Security

- Server-side header that tells your clients to always use HTTPS for your website
- Header MUST be served over HTTPS only.
- Examples:
  - Strict-Transport-Security max-age=604800;
  - Strict-Transport-Security "max-age=31536000; includeSubDomains"
- Real-life examples:
  - https://docs.google.com
  - https://void.gr :)

Secure Email Settings

- Run Wireshark and open your email client
- Read an email, can you see cleartext data on Wireshark ?
- Send an email, can you see cleartext data on Wireshark ?
- Change settings of your email client to support encryption:

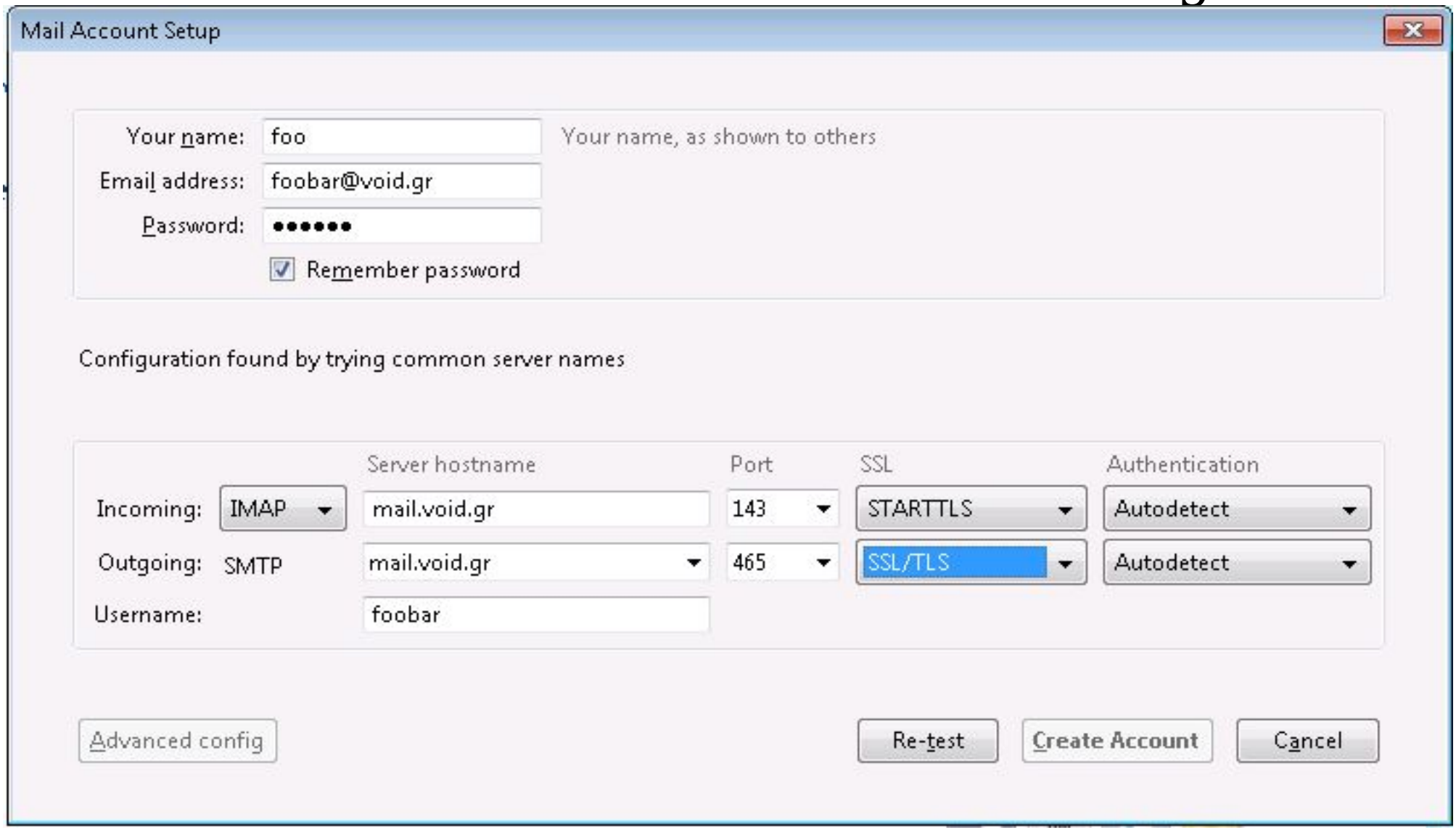
Protocol / Crypto Method	*No crypto* or ***STARTTLS***	***SSL***
SMTP	25	465
POP3	110	995
IMAP	143	993

Common Encryption options for mail clients

- **Never**: No encryption
- **TLS, if available**: Same port, client asks whether the server supports encryption, if not it continues *without* encryption.
- **STARTTLS**: Same port, client asks whether the server supports encryption, if not it doesn't continue (*)
- **SSL**: Different port, mandatory encryption (*)

(*) → Use these, avoid others!

Thunderbird Secure account settings



Instant Messaging

- **MSN Messenger/Yahoo! Messenger** do not support encrypted connections. **AVOID at all costs**!

```
▽ MSN Messenger Service
    MSG 31 A 206\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    User-Agent: pidgin/2.7.3\r\n
    X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; PF=0; RL=0\r\n
    \r\n
    omg my passwords are cleartext!
```

```
0000  00 1d 1c 01 57 f5 00 22  41 1e d8 06 08 00 45 00   ....W.." A.....E.
0010  01 10 a4 2f 40 00 40 06  56 10 c0 a8 01 5f 40 04   .../@.@. V...._@.
0020  3d 9d 96 21 07 47 d5 ab  37 45 18 33 01 a7 80 18   =..!.G.. 7E.3....
0030  be 5a 40 ab 00 00 01 01  08 0a 09 65 26 fa 13 ce   .Z@..... ...e&...
0040  81 9b 4d 53 47 20 33 31  20 41 20 32 30 36 0d 0a   ..MSG 31  A 206..
0050  4d 49 4d 45 2d 56 65 72  73 69 6f 6e 3a 20 31 2e   MIME-Ver sion: 1.
0060  30 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   0..Conte nt-Type:
0070  20 74 65 78 74 2f 70 6c  61 69 6e 3b 20 63 68 61    text/pl ain; cha
0080  72 73 65 74 3d 55 54 46  2d 38 0d 0a 55 73 65 72   rset=UTF -8..User
0090  2d 41 67 65 6e 74 3a 20  70 69 64 67 69 6e 2f 32   -Agent:  pidgin/2
00a0  2e 37 2e 33 0d 0a 58 2d  4d 4d 53 2d 49 4d 2d 46   .7.3..X- MMS-IM-F
00b0  6f 72 6d 61 74 3a 20 46  4e 3d 53 65 67 6f 65 25   ormat: F N=Segoe%
00c0  32 30 55 49 3b 20 45 46  3d 3b 20 43 4f 3d 30 3b   20UI; EF =; CO=0;
00d0  20 50 46 3d 30 3b 20 52  4c 3d 30 0d 0a 0d 0a 6f    PF=0; R L=0....o
00e0  6d 67 20 6d 79 20 70 61  73 73 77 6f 72 64 73 20   mg my pa sswords
00f0  61 72 65 20 63 6c 65 61  72 74 65 78 74 21 20 09   are clea rtext! .
```

Instant Messaging

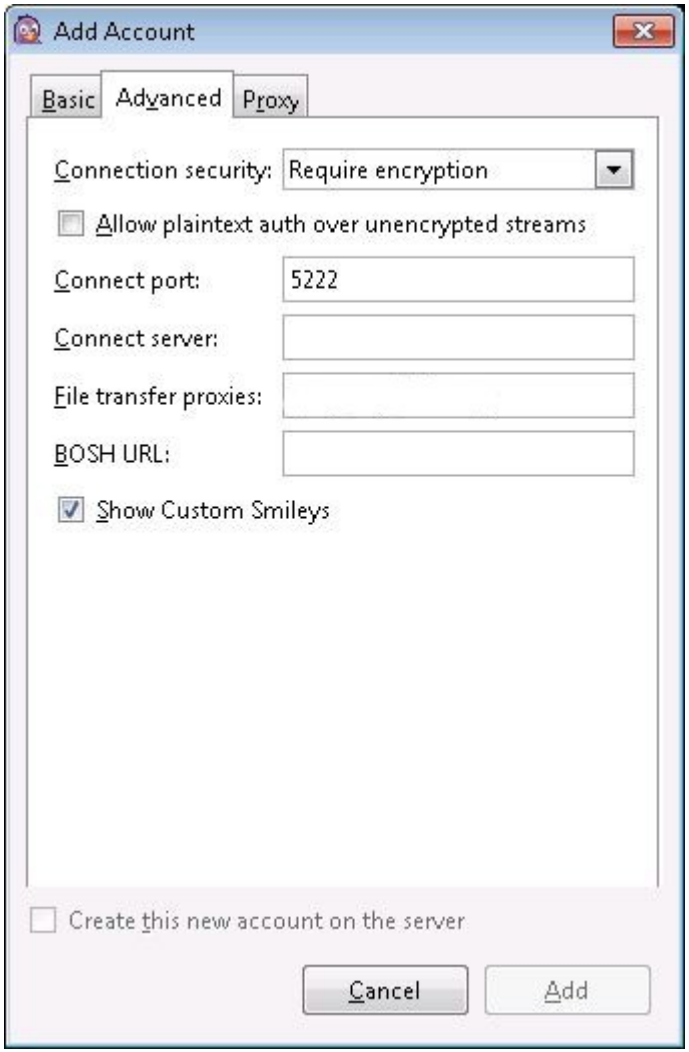
- Run Wireshark
- Talk to some friend over MSN/Yahoo!/Jabber
- Can you see **ANY** cleartext data being exchanged ? **So can others!**

Instant Messaging

- **Avoid using Skype**
  - Did Skype Give a Private Company Data on Teen WikiLeaks Supporter Without a Warrant?
- **Avoid** platforms that do **server-side logging** of chats (e.g. Facebook).
  - Google Talk* → Gmail→Settings→Chat→Never Save Chat History
- Prefer IM platforms that support the **XMPP protocol** (Jabber, Google Talk*). Open source/Open Standards.

Pidgin settings for Google Talk/Jabber

- "Connection Security":
  - **Require Encryption** (*)
  - ~~Use encryption if available~~
  - Use old-style SSL (different port: 5223)
- **Remove** "File Transfer Proxies"



Athens CryptoParty #0

Links:

- All these included at the slides

  +

- https://ssd.eff.org/ Surveillance Self-Defence
- https://skytal.es

Athens CryptoParty #0

Thanks!

Questions ?