[StuCo 98008]
GNU/Linux for Beginners

Session 11

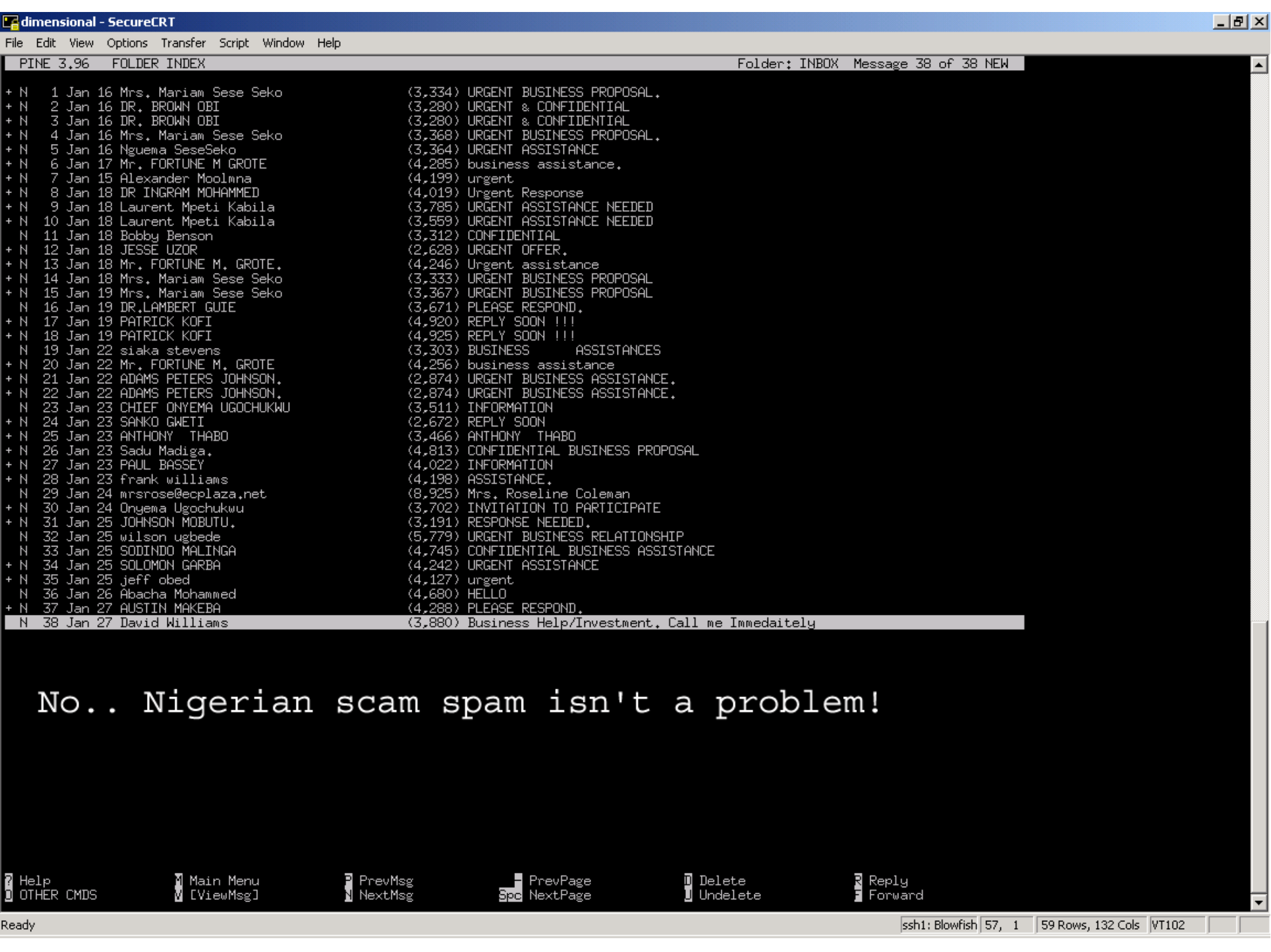
Privacy

By the end of this lecture you will know

- The ways by which commercial organizations and spammers collect your personal information
- How to defend your private information
- Settings/plugins of common GNU/Linux applications that help you strike a balance between usability and privacy

Privacy Violations

- Spam email
  - Spammers trying to sell you Viagra, “more confidence”, dates with Britney Spears, etc.
  - M$-assisted worms that bombard your mailbox and attempt to infect your computer
  - Scam email that costs lots of money (Nigerian spam)
- Targeted advertising
  - Implies that your online behavior is tracked
  - Consumer behavior patterns
  - “Minority Report”-like “Hi Alex, welcome back!”


dimensional - SecureCRT
File Edit View Options Transfer Script Window Help
PINE 3.96 FOLDER INDEX Folder: INBOX Message 38 of 38 NEW
+ N 1 Jan 16 Mrs. Mariam Sese Seko (3,334) URGENT BUSINESS PROPOSAL.
+ N 2 Jan 16 DR. BROWN OBI (3,280) URGENT & CONFIDENTIAL
+ N 3 Jan 16 DR. BROWN OBI (3,280) URGENT & CONFIDENTIAL
+ N 4 Jan 16 Mrs. Mariam Sese Seko (3,368) URGENT BUSINESS PROPOSAL.
+ N 5 Jan 16 Nguema SeseSeko (3,364) URGENT ASSISTANCE
+ N 6 Jan 17 Mr. FORTUNE M GROTE (4,285) business assistance.
+ N 7 Jan 15 Alexander Moolmna (4,199) urgent
+ N 8 Jan 18 DR INGRAM MOHAMMED (4,019) Urgent Response
+ N 9 Jan 18 Laurent Mpeti Kabila (3,785) URGENT ASSISTANCE NEEDED
+ N 10 Jan 18 Laurent Mpeti Kabila (3,559) URGENT ASSISTANCE NEEDED
N 11 Jan 18 Bobby Benson (3,312) CONFIDENTIAL
+ N 12 Jan 18 JESSE UZOR (2,628) URGENT OFFER.
+ N 13 Jan 18 Mr. FORTUNE M. GROTE. (4,246) Urgent assistance
+ N 14 Jan 18 Mrs. Mariam Sese Seko (3,333) URGENT BUSINESS PROPOSAL
+ N 15 Jan 19 Mrs. Mariam Sese Seko (3,367) URGENT BUSINESS PROPOSAL
N 16 Jan 19 DR.LAMBERT GUIE (3,671) PLEASE RESPOND.
+ N 17 Jan 19 PATRICK KOFI (4,920) REPLY SOON !!!
+ N 18 Jan 19 PATRICK KOFI (4,925) REPLY SOON !!!
N 19 Jan 22 siaka stevens (3,303) BUSINESS ASSISTANCES
+ N 20 Jan 22 Mr. FORTUNE M. GROTE (4,256) business assistance
+ N 21 Jan 22 ADAMS PETERS JOHNSON. (2,874) URGENT BUSINESS ASSISTANCE.
+ N 22 Jan 22 ADAMS PETERS JOHNSON. (2,874) URGENT BUSINESS ASSISTANCE.
N 23 Jan 23 CHIEF ONYEMA UGOCHUKWU (3,511) INFORMATION
+ N 24 Jan 23 SANKO GWETI (2,672) REPLY SOON
+ N 25 Jan 23 ANTHONY THABO (3,466) ANTHONY THABO
+ N 26 Jan 23 Sadu Madiga. (4,813) CONFIDENTIAL BUSINESS PROPOSAL
+ N 27 Jan 23 PAUL BASSEY (4,022) INFORMATION
+ N 28 Jan 23 frank williams (4,198) ASSISTANCE.
N 29 Jan 24 mrsrose@ecplaza.net (8,925) Mrs. Roseline Coleman
+ N 30 Jan 24 Onyema Ugochukwu (3,702) INVITATION TO PARTICIPATE
+ N 31 Jan 25 JOHNSON MOBUTU. (3,191) RESPONSE NEEDED.
N 32 Jan 25 wilson ugbede (5,779) URGENT BUSINESS RELATIONSHIP
N 33 Jan 25 SODINDO MALINGA (4,745) CONFIDENTIAL BUSINESS ASSISTANCE
+ N 34 Jan 25 SOLOMON GARBA (4,242) URGENT ASSISTANCE
+ N 35 Jan 25 jeff obed (4,127) urgent
N 36 Jan 26 Abacha Mohammed (4,680) HELLO
+ N 37 Jan 27 AUSTIN MAKEBA (4,288) PLEASE RESPOND.
N 38 Jan 27 David Williams (3,880) Business Help/Investment. Call me Immedaitely
No.. Nigerian scam spam isn't a problem!
? Help
O OTHER CMDS
M Main Menu
V [ViewMsg]
P PrevMsg
N NextMsg
- PrevPage
Spc NextPage
D Delete
U Undelete
R Reply
F Forward
Ready
ssh1: Blowfish
57, 1
59 Rows, 132 Cols
VT102

Why Do I Get Spam?

- You have posted to public mailing lists/newsgroups
  - Such lists/newsgroups are archived, and spammer bots (scripts) read through them to harvest legitimate email addresses.
- You have used online services that required an email
  - Service providers regularly sell the personal information of their subscribers
- You have received email from a friend with a free web mail address
  - Outgoing email addresses are harvested and sold to spammers

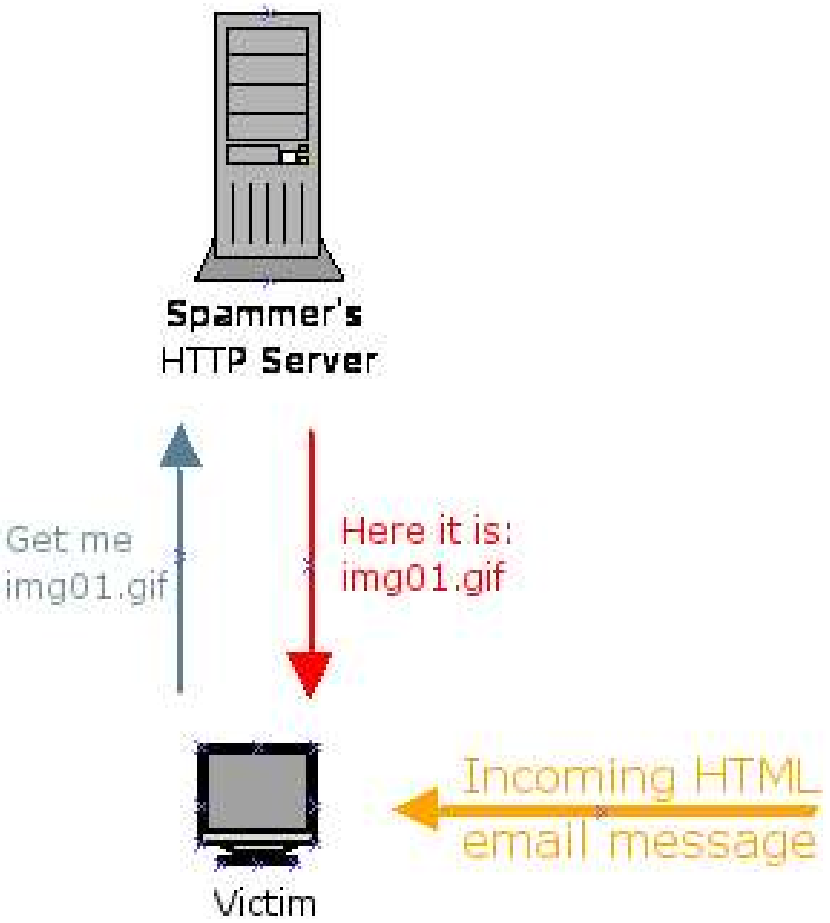
Defenses Against Spam

- **Proactive**
  - Don't give out your real information unless you **must**
  - Use a “junk” account for online registrations
  - Don't accept HTML email
  - Use timestamped addresses (apapadop+rh7Jul02@cmu.edu)
- **Reactive**
  - Use spam filtering software like SpamAssassin
  - Never click on “click here to unregister” links

The Joys of HTML email

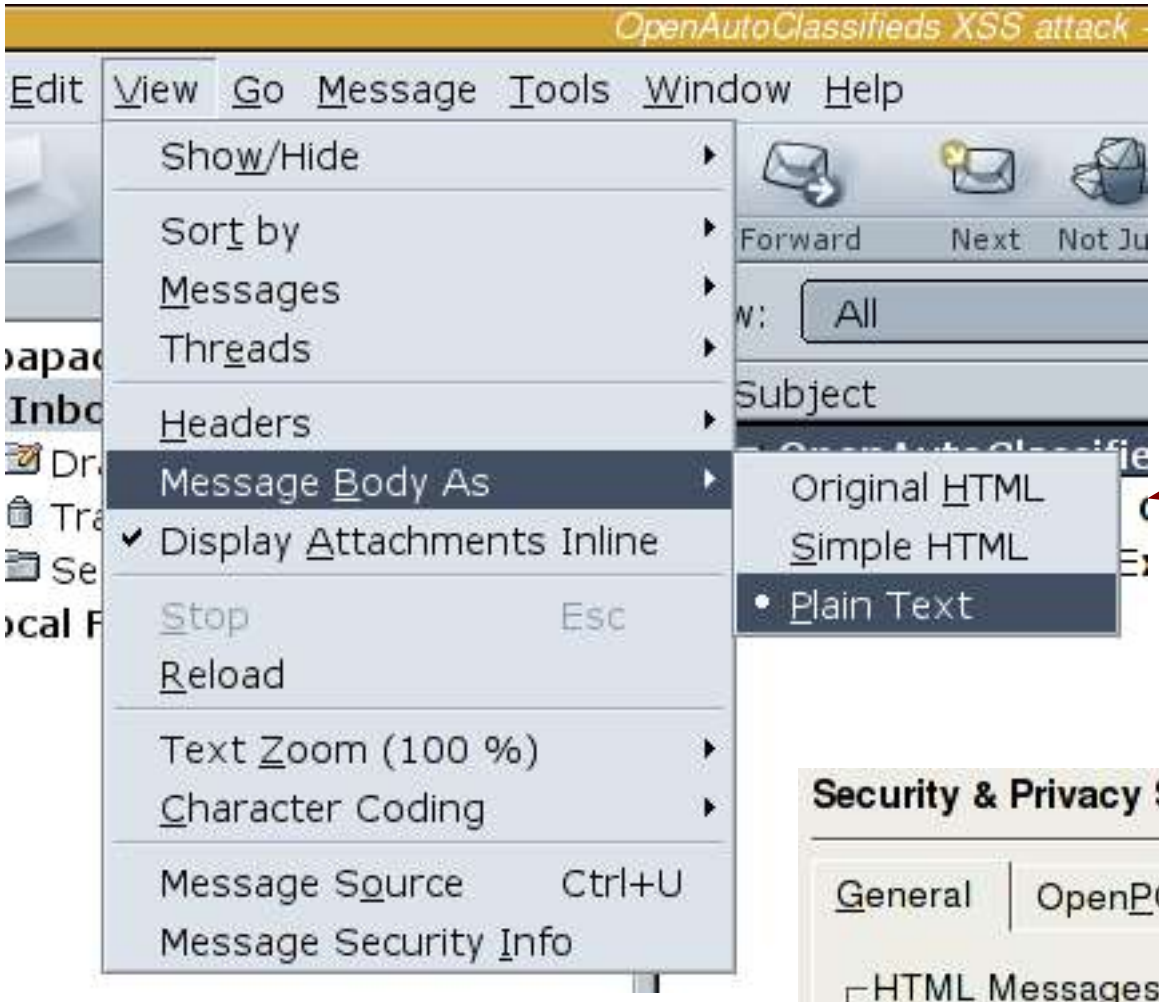
- Web browser is typically invoked
  - All web browser vulnerabilities applicable
- **Web bugs** (remote transparent 1x1 images)
  - You're in spammer's HTTP server logs
  - Good email address, keep for future spamming
  - All your IPs/timestamps are belong to us
- **JavaScript** and friends
  - No legitimate use
  - Malicious code execution (worms, trojans)

What Happens When You Get An HTML email?



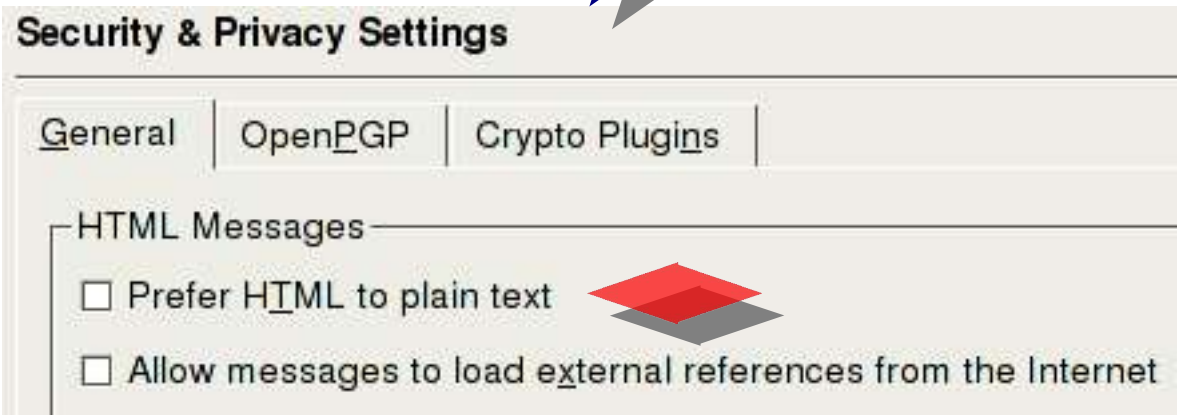
1. Client tries to render the HTML
2. Remote elements are loaded from the network
3. **Busted** – you're in spammer's logs

Turning Off HTML email

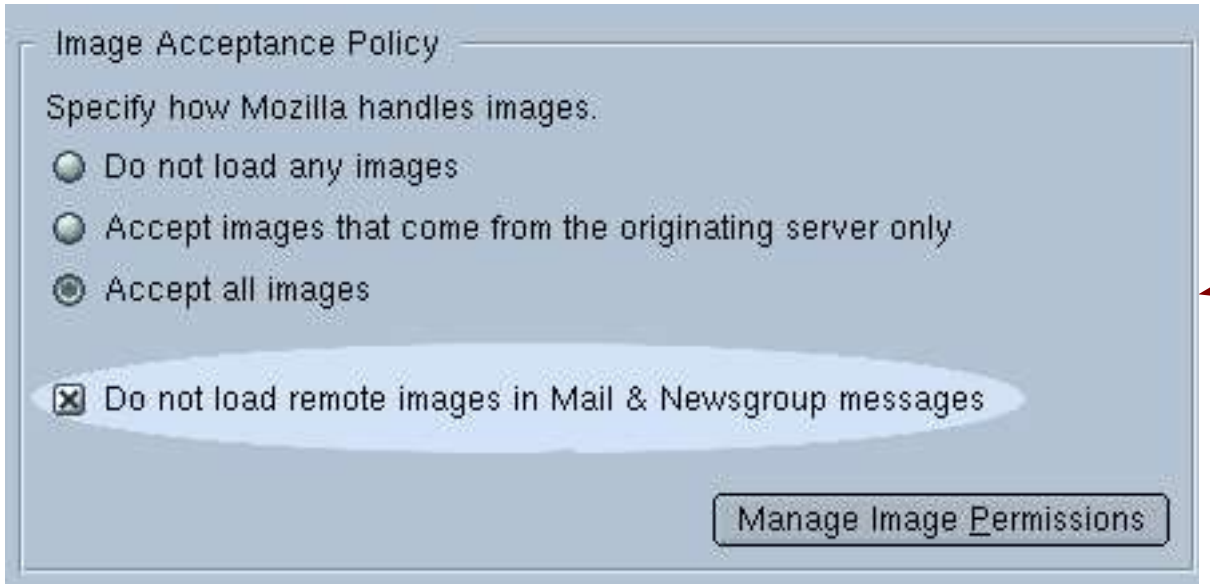


Mozilla

KMail

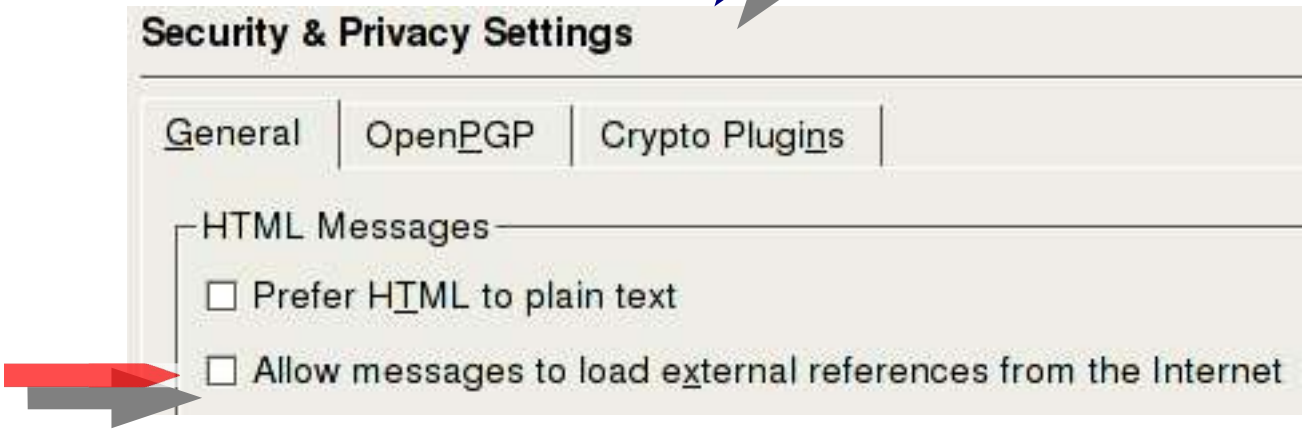


Getting Rid of Web Bugs



Mozilla

KMail



Tracking People on the Web

- The “referer” field
  - Where did this visitor come from?
- Cookies
  - Uniquely identifiable consumers
- Banner ads
  - Profiling

The Good Cookies

- Small text files stored on your local machine
- They usually keep useful information for a specific site – e.g. **lang=el** for a multi-language site
- Necessary for web authentication, since HTTP is stateless
- Theoretically not accessed by anyone else but the site that put them there.

Misuse of Cookies

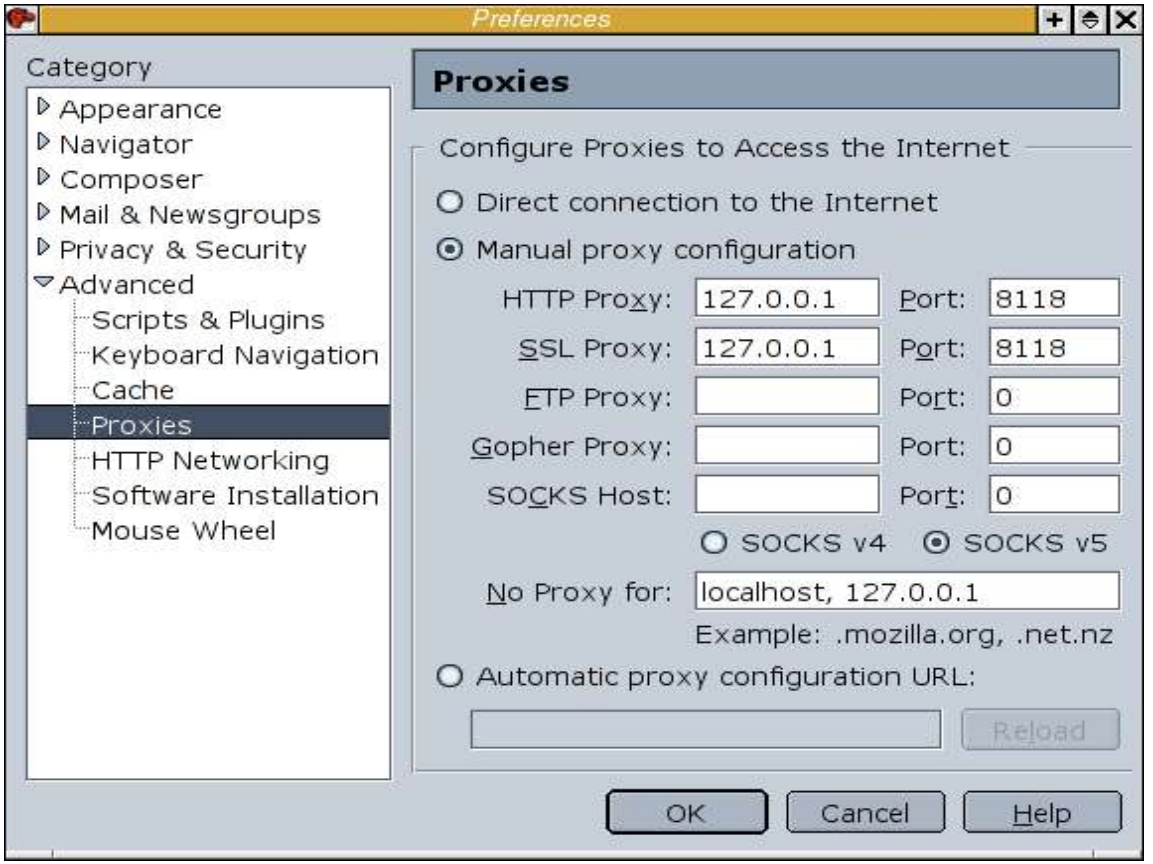
- **Consumer profiling** networks like DoubleClick
  - Cookies combined with banner ads
  - Why do banners always point to so long URLs?
- Accessing **cookies of other domains**
- Everyone gives you a cookies nowadays. Do you need them?
- **Cookies are only necessary for authentication**

Defenses Against Cookie Misuse

- **User decides** to accept/reject cookies per domain
  - Actually works after a while
  - Always use the “remember my choice” feature
- **Expire all** cookies when I exit my browser
  - Hassle-free web browsing
  - Keeps all sites happy
  - Acceptable, as long as you quit your browser often

Privoxy – Anonymizing HTTP Proxy

- All HTTP requests + replies go through Privoxy
- It strips all cookies / banner ads / popups
- Breaks some sites




```
MozillaFi 17711    alex   43u  IPv4 1072698
MozillaFi 17711    alex   46u  IPv4 1072700
MozillaFi 17711    alex   48u  IPv4 1072701
MozillaFi 21481    alex   40u  IPv4 1072693
MozillaFi 21481    alex   43u  IPv4 1072698
MozillaFi 21481    alex   46u  IPv4 1072700
MozillaFi 21481    alex   48u  IPv4 1072701
privoxy   21623 privoxy    3u  IPv4 1043444
privoxy   21623 privoxy    4u  IPv4 1072689
privoxy   21623 privoxy    7u  IPv4 1072702
privoxy   21623 privoxy    8u  IPv4 1072695
```

```
TCP 127.0.0.1:33022->127.0.0.1:8118 (ESTABLISHED)
TCP 127.0.0.1:33023->127.0.0.1:8118 (ESTABLISHED)
TCP 127.0.0.1:33024->127.0.0.1:8118 (ESTABLISHED)
TCP 127.0.0.1:33021->127.0.0.1:8118 (ESTABLISHED)
TCP 127.0.0.1:33022->127.0.0.1:8118 (ESTABLISHED)
TCP 127.0.0.1:33023->127.0.0.1:8118 (ESTABLISHED)
TCP 127.0.0.1:33024->127.0.0.1:8118 (ESTABLISHED)
TCP 127.0.0.1:8118 (LISTEN)
TCP 127.0.0.1:8118->127.0.0.1:33021 (ESTABLISHED)
TCP 141.151.136.150:33025->195.134.99.76:www (ESTABLISHED)
TCP 127.0.0.1:8118->127.0.0.1:33022 (ESTABLISHED)
```

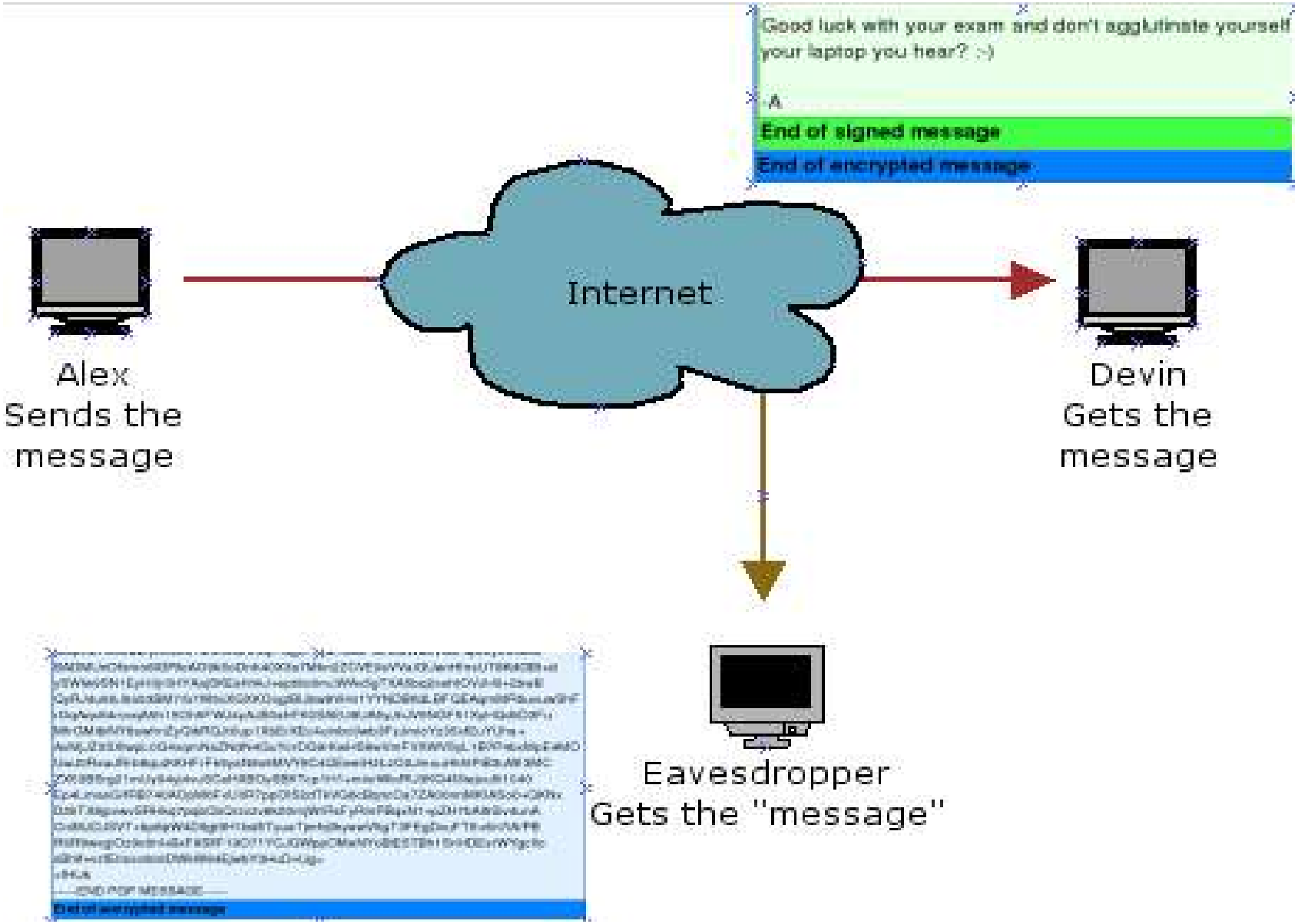
Email Encryption

- How?
  - **P**ublic **K**ey **I**nfrastructure
  - OpenPGP standard (RFC2440)
- Why?
  - **Confidentiality** (third parties **cannot read** your email)
  - **Integrity** (message is not **altered** while in transit)
  - **Authentication** (I **know** who sent the message)

Public Key Crypto

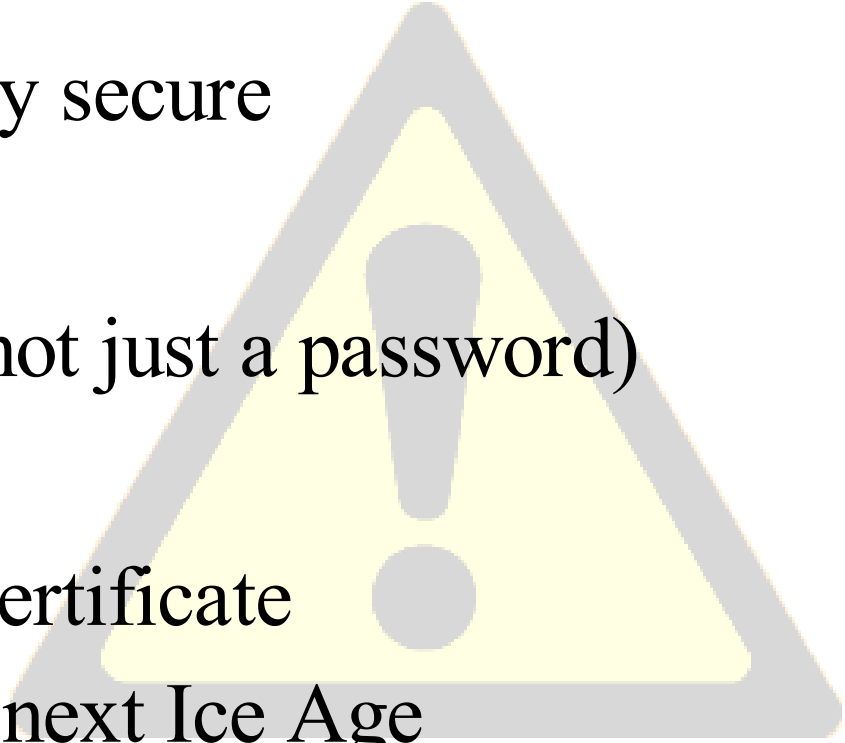
- Alice has a **private** and a **public** key. So does Bob.
- They both post their public keys on a **key server**.
- Alice gets Bob's public key from the server.
- Alice uses Bob's public key to **encrypt** a message to him.
- Alice **signs** the message with her private key.
- Bob gets the message. He uses his private key to **decrypt** the message, and reads it. No one else could have read it.
- Bob uses Alice's public key to **verify her signature**. No one else could have signed it, so the message is from Alice.

An Encrypted Message



PKI Pitfalls

- Getting a **corrupt public key**
  - Always check the fingerprint, e.g.
    3DAD 8435 DB52 F17B 640F D78C 8260 0CC1 0B75 8265
  - By phone call, or face-to-face verification
- Not keeping your **private** key secure
  - Secure your machine
  - Use a strong passphrase (not just a password)
- Key **mismanagement**
  - Always issue revocation certificate
  - Set expiry date before the next Ice Age



Creating Your Own Keys - GnuPG

1. $ gpg --gen-key
2. $ gpg --list-keys
3. $ gpg -o revcert.asc --gen-revoke <myID>
4. $ gpg --send-keys --keyserver pgp.mit.edu
5. Go to http://pgp.mit.edu to verify your key
6. $ gpg --fingerprint <myID>
7. $ gpg --import revcert.asc
8. $ gpg --send-keys --keyserver pgp.mit.edu
9. Go to http://pgp.mit.edu to check proper revocation

Crypto – Email Client Integration

- KMail: Native GnuPG support
- Mozilla: EnigMail plugin
- Other mail clients that support OpenPGP
  - Mutt
  - Pine
  - Sylpheed
  - Mozilla ThunderBird

Encrypting Local Files With GnuPG

- **$ gpg --encrypt --recipient** <myID> <filename>
  - Encrypts and compresses the file
  - Creates <filename>.gpg
- **$ gpg --decrypt --output** <filename> <filename>.gpg
  - Decrypts the contents of <filename>.gpg into the file <filename>