Security Simplified(?)

hint: Not really, no!

Fundamentals

What is security?

Why security?

How to be secure?

What is security?

You don't want to lose stuff

You don't want somebody to look at your stuff

You don't want somebody to alter stuff you send to your friend

What is security? contd..

You don't want somebody to pretend to be you and communicate with your friend

And we all know that guy who claims he never sent stuff he sent you

Fancy words..

Not losing stuff - Availability

Stuff is not altered - Integrity

No-one looks at stuff - Confidentiality

Certainty of who sent stuff- Authenticity

Can’t deny having sent stuff - Non-repudiation

Being secure

Use common sense!

Do not share identifying information

Do not save passwords

Do not be stupid on social networking sites

Security vs. Convenience

Being secure - contd..

Phishing and vishing

Password123 and P@$$W0rd!23 don't count

And no, you have NOT been left with a few hundred million nigerian bucks by the dying king and nobody's seeking for your custody of the money

Some tips

Use a better operating system

Use a better browser

Use HTTPS / TLS everywhere

tips contd..

Do you use IE 6? Please kill yourself!

Using FaceBook

Using Chat systems

Using Email (GMAIL, etc)

Technical shit

Data in-situ vs. Data in-transit

Public Key and Private Key Encryption

OpenSSL AES

```
openssl aes-256-cbc -in attack-plan.txt -out message.enc
openssl aes-256-cbc -d -in message.enc -out plain-text.txt
```

Cryptsetup, LUKS

Data in-transit

Browsing – HTTPS

- HTTPS Everywhere

Email - GNU Privacy Guard (GPG)

- GPG4Win

Webchat - OTR (Not the Gmail OTR!)

Data in-transit

Check out cryptocat

Use TOR (Download the browser bundle)

Use TAILS (tails.boum.org)

Use better phones

Snake oil

Security by obscurity

Proprietary algorithms

Military Grade encryption

Bulletproof Security

Ethical hacking

Script kiddie stuff

more snake oil

Keys that are too long (>4098)

Appeal to authority

Complex terminology that can’t be looked up

tall claims

“Encryptor 4.0 uses a unique in-house developed incremental base shift algorithm. Decryption is practically impossible, even if someone manages to reverse engineer our program to obtain the algorithm, the decryption of a file depends on the exact password (encryption key). Even if someone is guessing the encryption key the file will only be decrypted correctly if the encryption key is 100 percent correct.”

Good security

Open algorithms

Practical and understandable

‘100% secure’ is a myth.

Standards & Protocols

Peer review

Trust establishment

Q & A

Free Software Foundation, Tamil Nadu

http://fsftn.org

Teek Hai