RECENT NEWS

"Hacker's Work Is a Form Of Participation in the Work of God in Creation."

-By,
Father Antonio Sapadaro (Vatican)

Do You?


+ O.S. User Accounts
+ Browse Web
+ Use Web Services
+ Use Computer Networks Any Way
+ Have Any Form Of Binary Data


You Are Not Secure If You Don't...
+ Use Strong Passwords 'n Keep Them Safe
+ Browse Web In Safe Browsers
+ Use SSL-ified Web Services
+ Use Patched Name Servers
+ Keep Your Data Protected

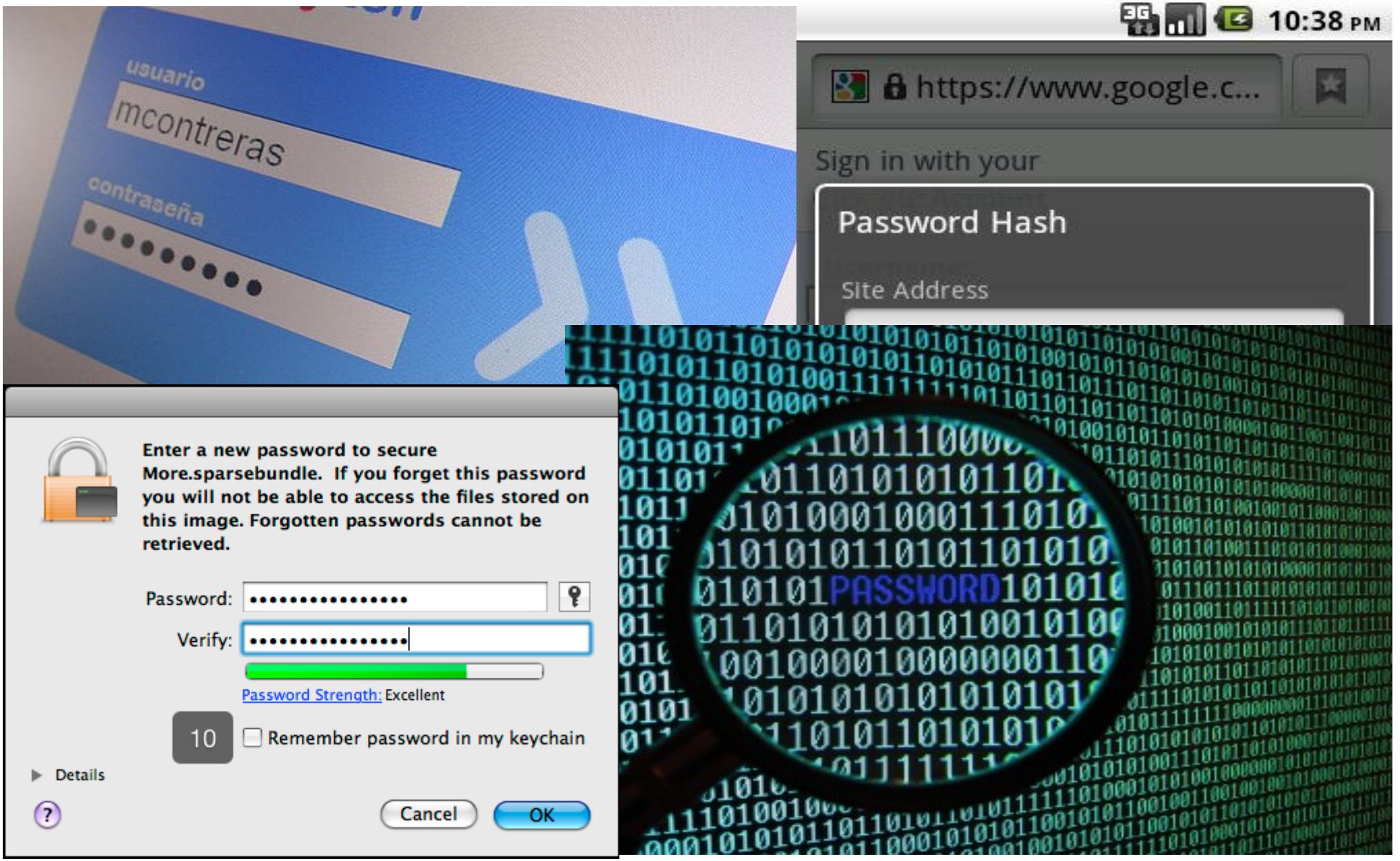

You Are InSecure Even If You Did...
MARIN
FAIL
TensionNOT.com

InSecurity In Security

Security is just maintained... it's never achieved.

First Some history from Version 1

O.S. User Accounts



Bypass Account Protection

Vaccinated Browsers

Browsing <Unknown> WWW

[+] SMBEnum

|=+ using 'file ://', 'res ://', 'resource ://'

Say, if it gains success accessing
'file:///c:/oracle/ora81/bin/orclcontainer.bmp'

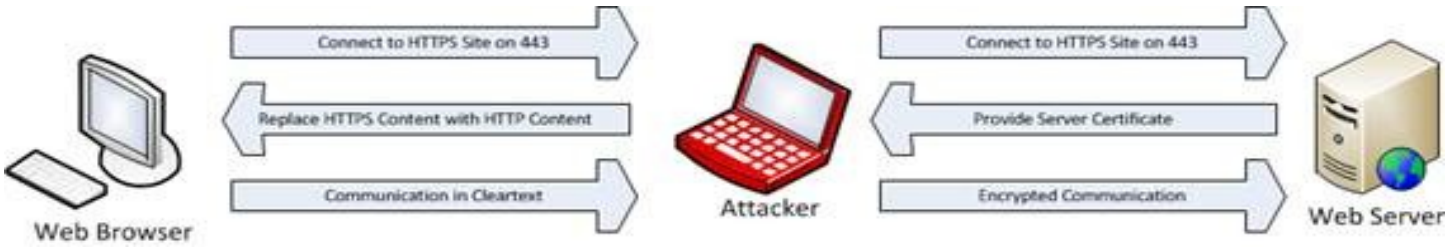
[+] ResTiming Attack

|=+ using 'res ://', 'resource ://' to execute

So, gains timing for different binaries &
Identify which exists

Protector of All

Defeating SSL



SSL Certificates

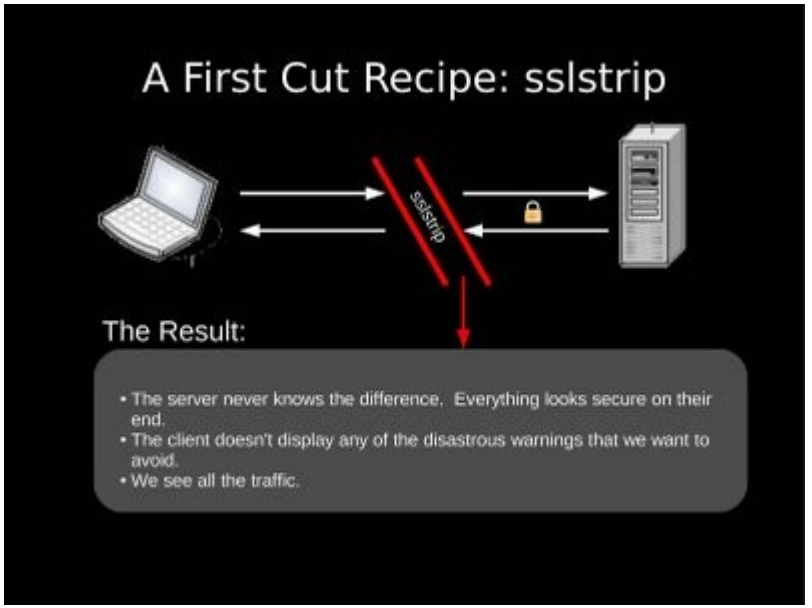
GeoTrust

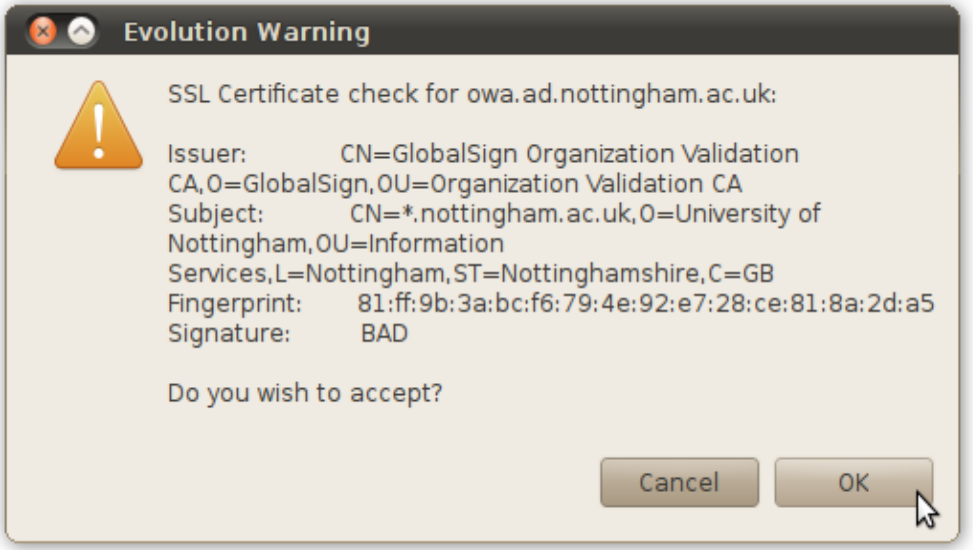
VeriSign

[] "Signing Authority" field in Digital Certificates

[] Tricking SSL Libraries with NULL Mod Certificates

[] **Online Certificate Revocation Policy** {ResponseStatus=3, ResponseBytes='' || SSL}





Basis Of All Networks

DNSSEC AINT ALL GOOD

[] Provides 'Origin Auth', 'Integrity Protection', PKI & even Auth· Denial of Data Existence

[] Still No 'Confidentiality' {basics of security} AND CPU-flooding is possible due to exhaustive cryptography

[] Variation of DNS Rebinding Attack presented at BH2010 still affected network

Data Forensics

TestDisk Data Recovery Utility

Data Forensic Hackers

[] Data Carving (Imaging RAM, Dig O·S·)

[] Dig Information from Files

[] Timestomp, Zipbomb

-=-

[] Mining Network Traffic for Files/Sessions

Now Some Mystery for Version 2

Hash-Crack on Steroids

Download latest version

Name	Version	md5sum	Date
oclHashcat	v0.25	7f8cc3e62b15345aa4c3cf6b6ee66374	2011.01.26

GPU Driver and SDK Requirements:

- NV users require at least ForceWare v260.x
- ATI users require at least Catalyst v10.12 + ATI Stream SDK v2.3 or Catalyst v10.12 APP version

Features

- **Free**
- **Multi-GPU (up to 16 gpus)**
- **Multi-Hash (up to 24 million hashes)**
- **Multi-OS (Linux & Windows native binaries)**
- **Multi-Platform (OpenCL & CUDA support)**
- **Multi-Algo (MD4, MD5, SHA1, DCC, NTLM, MySQL, ...)**
- **Fastest multihash MD5 cracker on NVidia cards**
- **Fastest multihash MD5 cracker on ATI 5xxx cards**
- **Supports wordlists (not limited to Brute-Force / Mask-Attack)**
- **Combines Dictionary-Attack with Mask-Attack to launch a Hybrid-Attack**
- Runs very cautious, you can still watch movies or play games while cracking
- Supports pause / resume
- The first and only GPU-based Fingerprint-Attack engine
- Includes hashcats entire rule engine to modify wordlists on start

hashcat
advanced
password
recovery

OpenCL

http://hashcat.net/oclhashcat/

'RSA' Theft & Threat

RSA

The Security Division of EMC

NETWITNESS

http://www.schneier.com/blog/archives/2011/03/rsa_security_in.html

Comodo Pwn3d Certs

```
1. Hello
2.
3. I'm writing this to the world, so you'll know more about me..
4.
5. At first I want to give some points, so you'll be sure I'm the hacker:
6.
7. I hacked Comodo from InstantSSL.it, their CEO's e-mail address mfpenco@mfpenco.com
8. Their Comodo username/password was: user: gtadmin password: [trimmed]
9. Their DB name was: globaltrust and instantsslcms
```

```
26. a) I'm not a group of hacker, I'm single hacker with experience of 1000 hackers, I'm single programmer
    with
27.
28. experience of 1000 programmers, I'm single planner/project manager with experience of 1000 project
29.
30. managers, so you are right, it's managed by a group of hackers, but it was only I with experience of
    1000
31.
32. hackers.
```

COMODO
Creating Trust Online®

JANAM FADAYE RAHBAR

http://www.wired.com/threatlevel/2011/03/comodo_hack/

OpenBSD 'n Backdoors

[]10yrs back FBI consulted NETSEC, CTO Perry

[]Lotz of code commit by NETSEC developers

[]Few daz back, Perry's NDA expired with FBI

[]Alleged backdoors in IPSEC Stack

[]FreeBSD inherited lotz code from OpenBSD

http://marc.info/?l=openbsd-tech&m=129236621626462&w=2

Samsung Key-log Conflict

SAMSUNG

http://arstechnica.com/hardware/news/2011/03/samsung-laptop-keylogger-almost-certainly-a-false-positive.ars

Who Is This Guy?

Family Named: AbhishekKr

Friends Call: ABK

g33k Handle: aBionic {@Twitter, @LinkedIn, @Facebook}

Itweet : http://www.twitter.com/aBionic

iBlog: http://abhishekkr.wordpress.com

Security Enthusiast; Working for ThoughtWorks Inc.; OpenSource Lover

My Crime Is That Of Curosity

Any Questions?