D’ ENLIGHTENMENT

Day to Day Security for
Business Managers, Users and SMEs

Jim Geovedi
jim.geovedi@bellua.com

“**Information Security** is about technology, policy, people and common sense”

“**Security** is a multifaceted word with many different connotations; it involves ***protecting*** an organization’s critical information ***from threats***”

dotslashjac

“**Securing your information** is a big issue that is ***getting more complex*** every day”

Information Security and the CSO

- Most organizations in the Asia Pacific region beginning to realize that security and continuity are important issues.
  - 40% IT Managers rated security as their highest priority.
- Security challenges are getting more complex.
  - Future trends include policy-enforced client security, identity management and the convergence of physical and virtual security.
- Delivering business resilience in an “always connected” global economy.

Information Security and the Organization

- Protection of an organization’s critical information.
  - Minimizing the risk posed by internal and external threats.
- Ultimately driven by business needs.
  - A balance between ***CONFIDENTIALITY,*** ***INTEGRITY*** and ***AVAILABILITY***.
- Internet has brought significant hazards.

“Even the best technology can fail”

Did Technology Fail?

- **YES!**
  - In spite of the best technology in place, security had been compromised.
- **NO!**
  - The technology did not fail to deliver, the breach was a human failure.

The Weakest Link

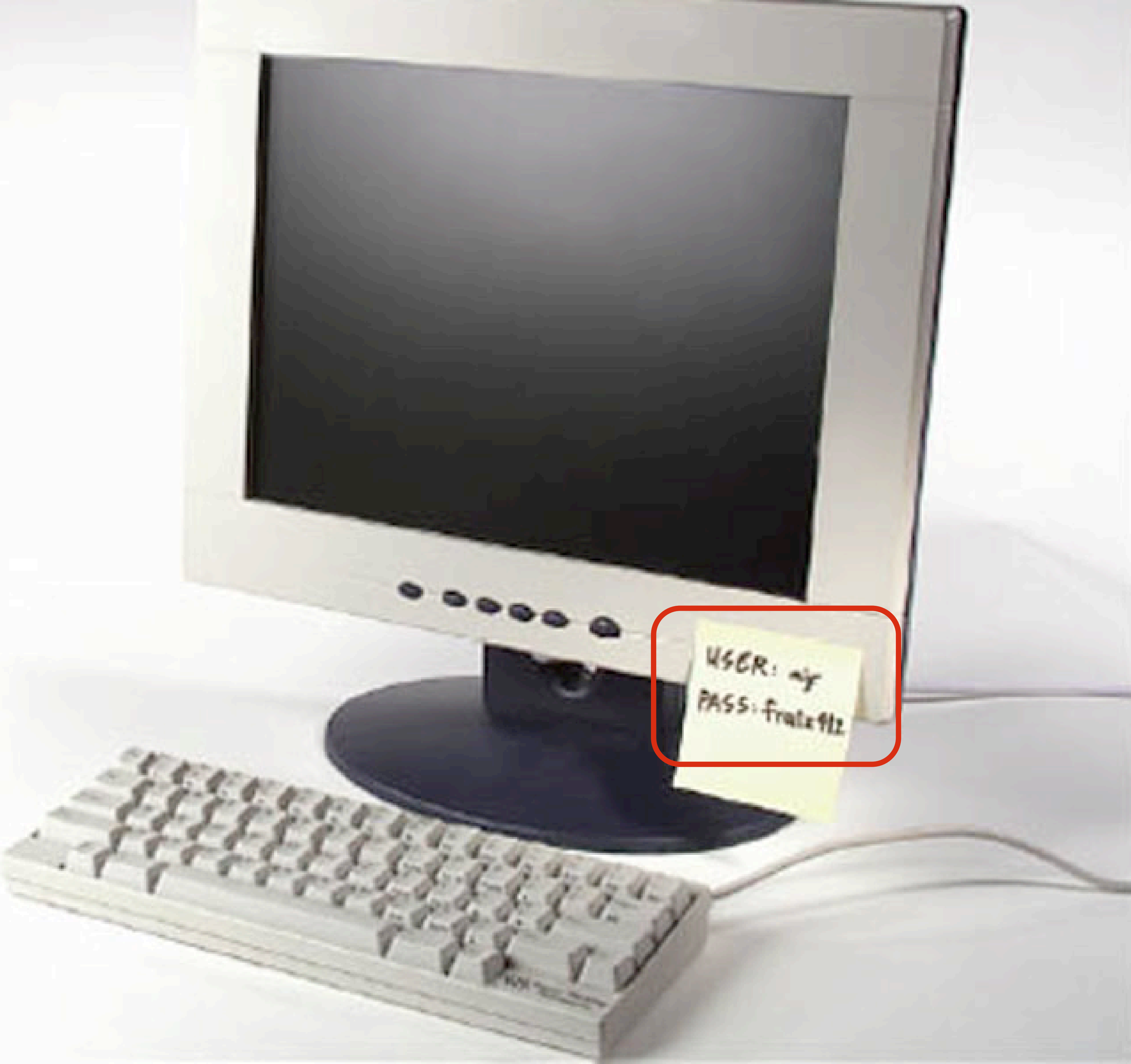
- The weakest link in security is ***the human element***.
    - **"We have met the enemy; and he is us".**
- A security program is effective only if:
    - Every individual in his/her respective capacity is security conscious.
    - Implements the information security policies of the organizations.

Seven Best Practices in Information Security

1. Have a defined information security policy.
2. Deny all, unless explicitly authorized and allowed.
3. Encrypt all data communicated over public connections.
4. Classify the information.
5. Use information-handling procedures based on the classifications.
6. Enforce access control.
7. Minimize, or eliminate exceptions to the rule.

Today **issues**

Put your stuff **online**.


USER: mjr
PASS: fraiz912

$3KuRe,P455w()rd!

Imm4/el8

Kd7!c@5d

T3mVNjtL

KyM0m!5aBych

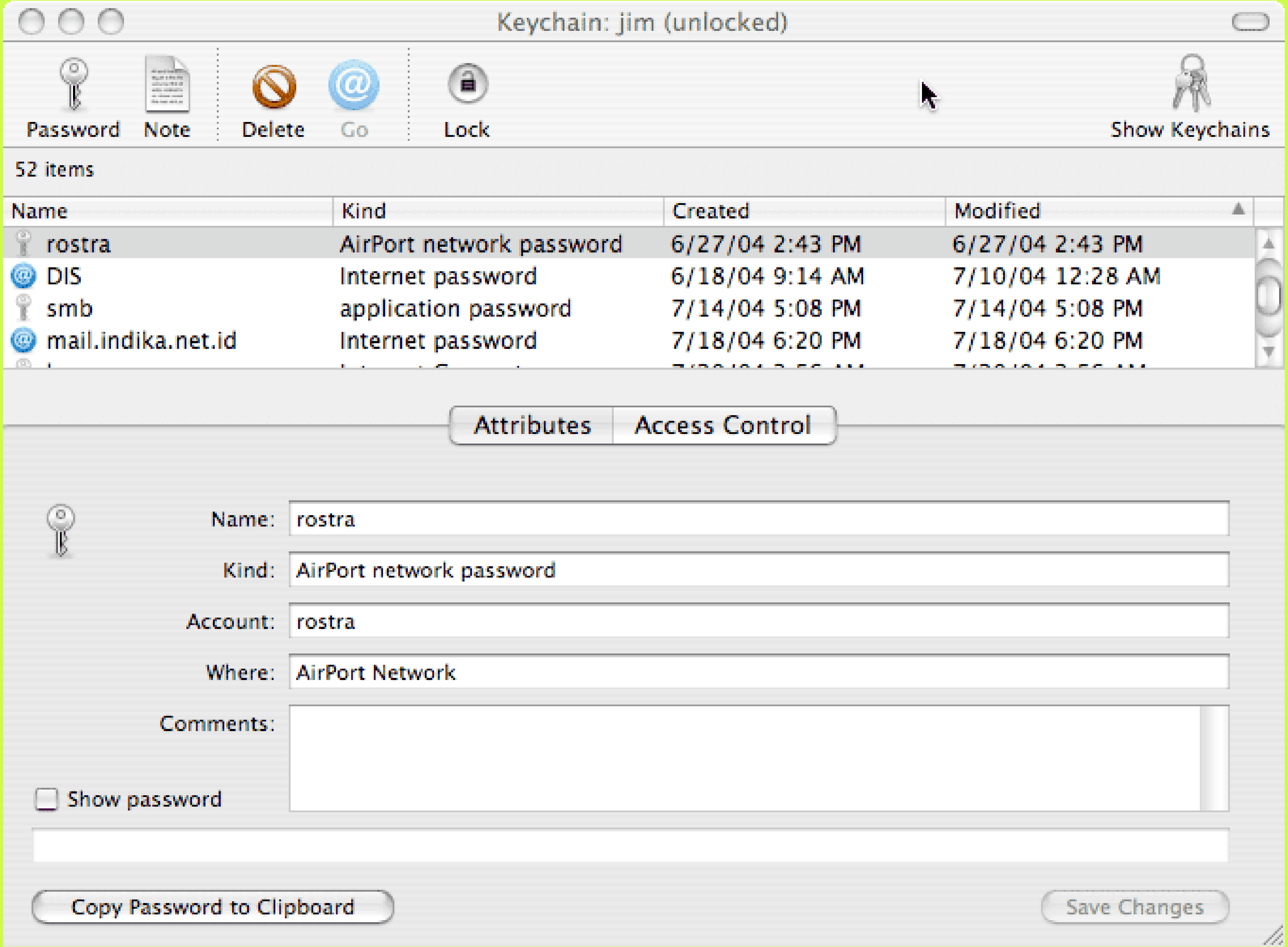
0280673

justenter

username

username123

dellon



Keychain: jim (unlocked)

52 items

Name	Kind	Created	Modified
rostra	AirPort network password	6/27/04 2:43 PM	6/27/04 2:43 PM
DIS	Internet password	6/18/04 9:14 AM	7/10/04 12:28 AM
smb	application password	7/14/04 5:08 PM	7/14/04 5:08 PM
mail.indika.net.id	Internet password	7/18/04 6:20 PM	7/18/04 6:20 PM

Name: rostra

Kind: AirPort network password

Account: rostra

Where: AirPort Network

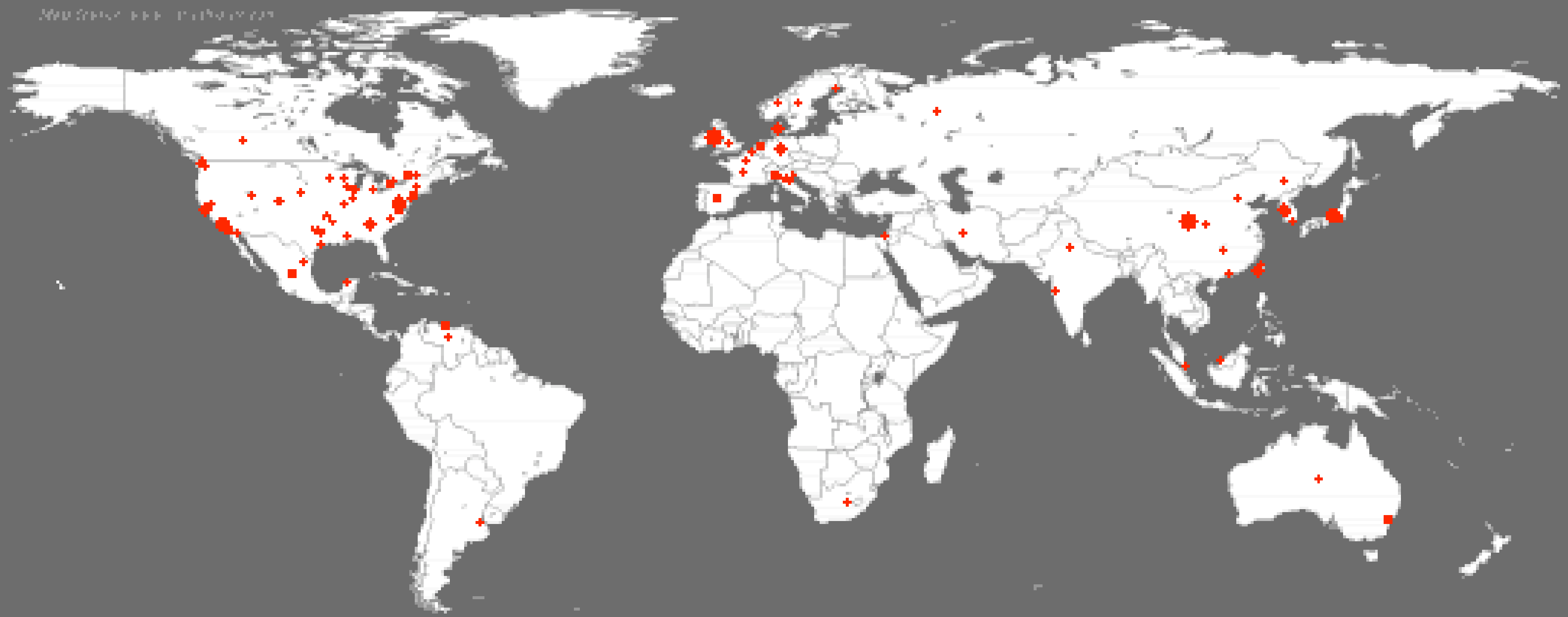
Comments:

☐ Show password

Zombies, Trojans, Bots, Worms

What have we wrought?

“Over 30,000 computers are *recruited* into **botnets** every day”



“***Malware*** is increasingly being designed to steal personal data, particularly financial information and passwords”

“Two of the most troublesome are **flash threats** and **self-mutating worms**”

Encryption

SSL / TLS

- Cryptographic security
- Interoperability
- Extensibility
- Relative efficiency

Practical use of SSL / TLS

- Web Mail
- Mail transport
- Secure login / ftp

PGP / GPG

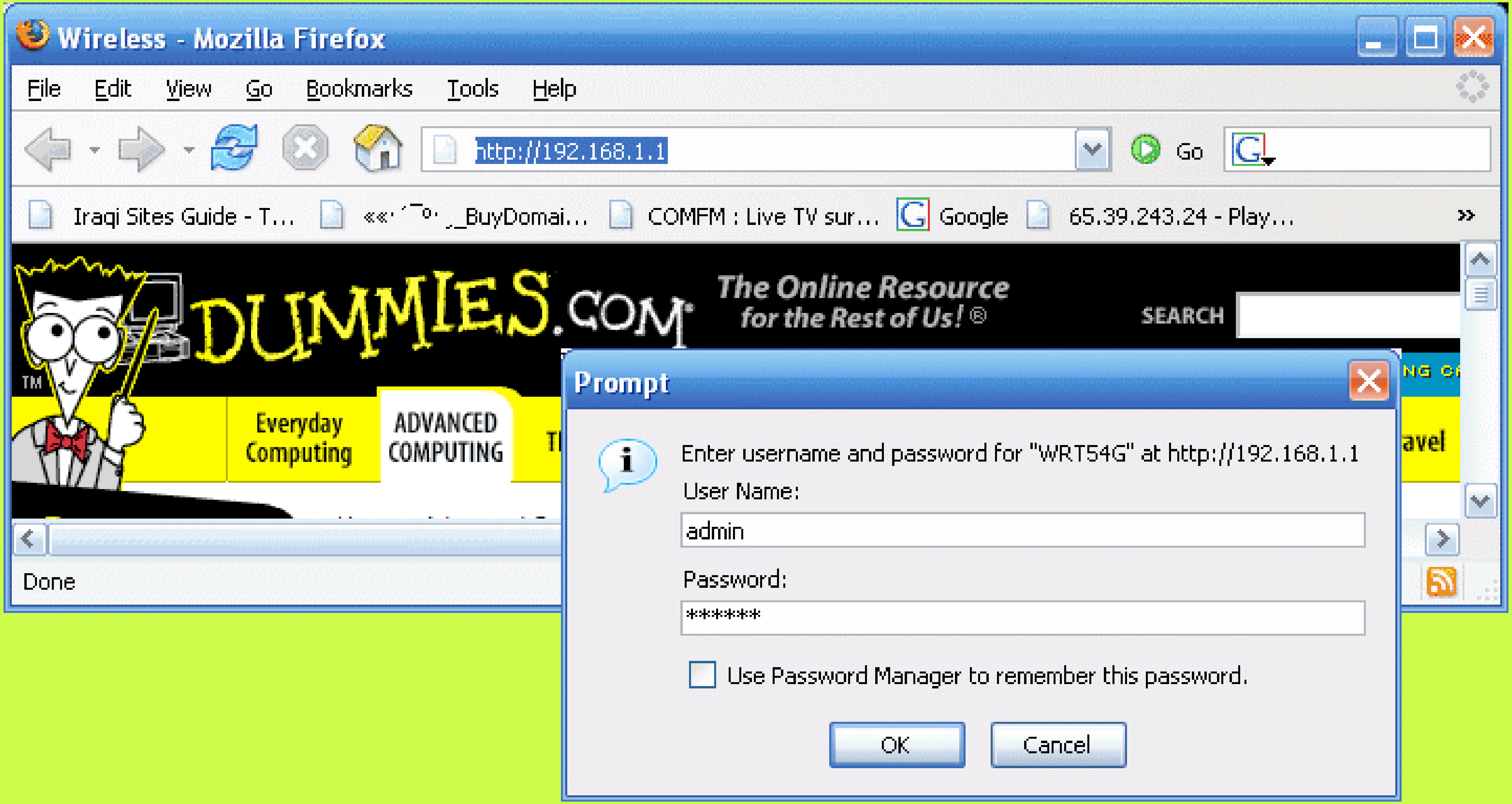
- http://www.pgp.com/
- http://web.mit.edu/network/pgp.html
- http://www.gnupg.org/

Disk **Encryption** Tool

Hard Disk Encryption

- http://directory.google.com/Top/Computers/Security/Products_and_Tools/Cryptography/Hard_Disk_Encryption/
- http://www.infoanarchy.org/wiki/index.php/Hard_Disk_Encryption

Wireless **Encryption**

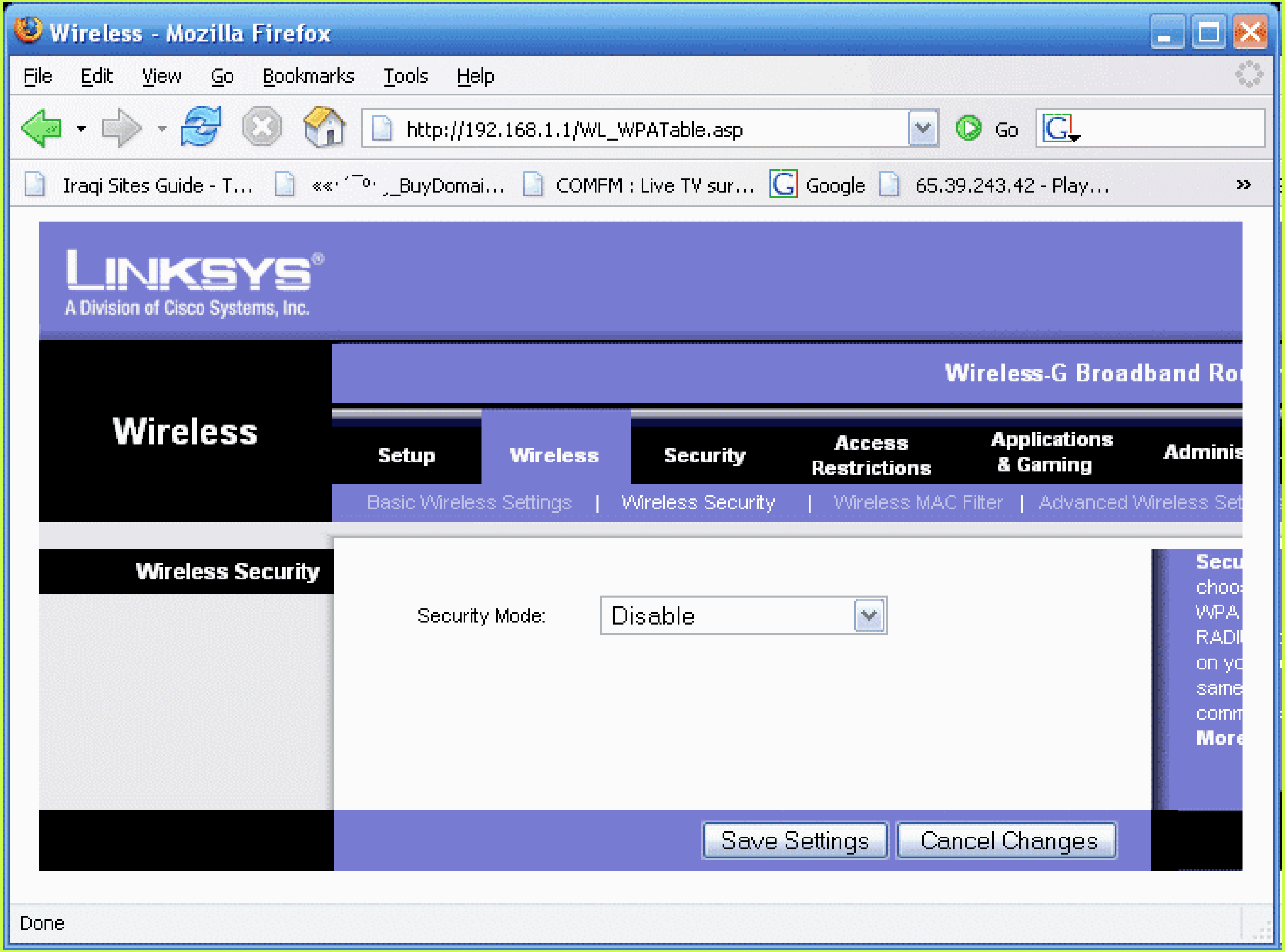


Enter username and password for "WRT54G" at http://192.168.1.1

User Name: admin

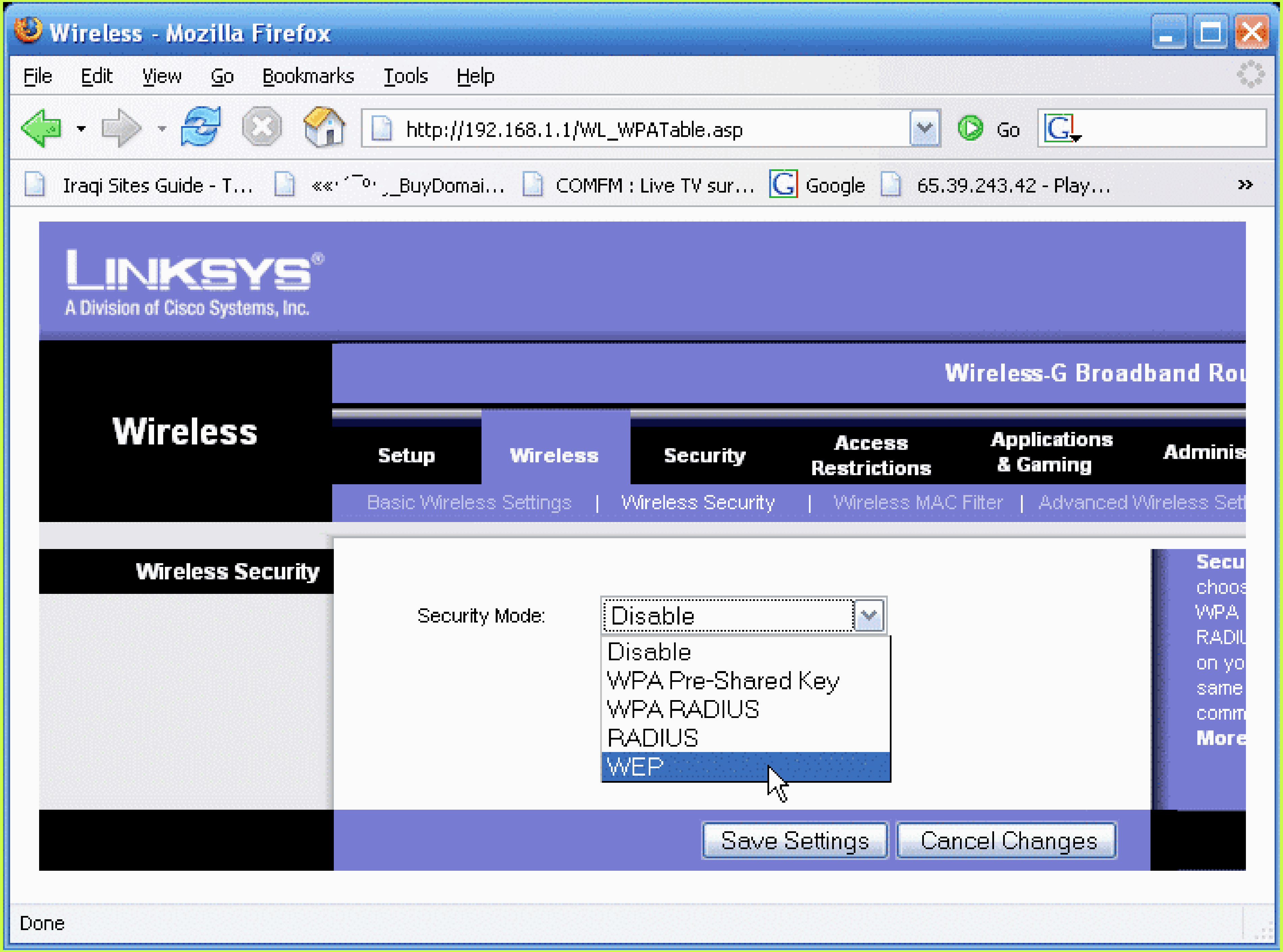
Password: *******

□ Use Password Manager to remember this password.

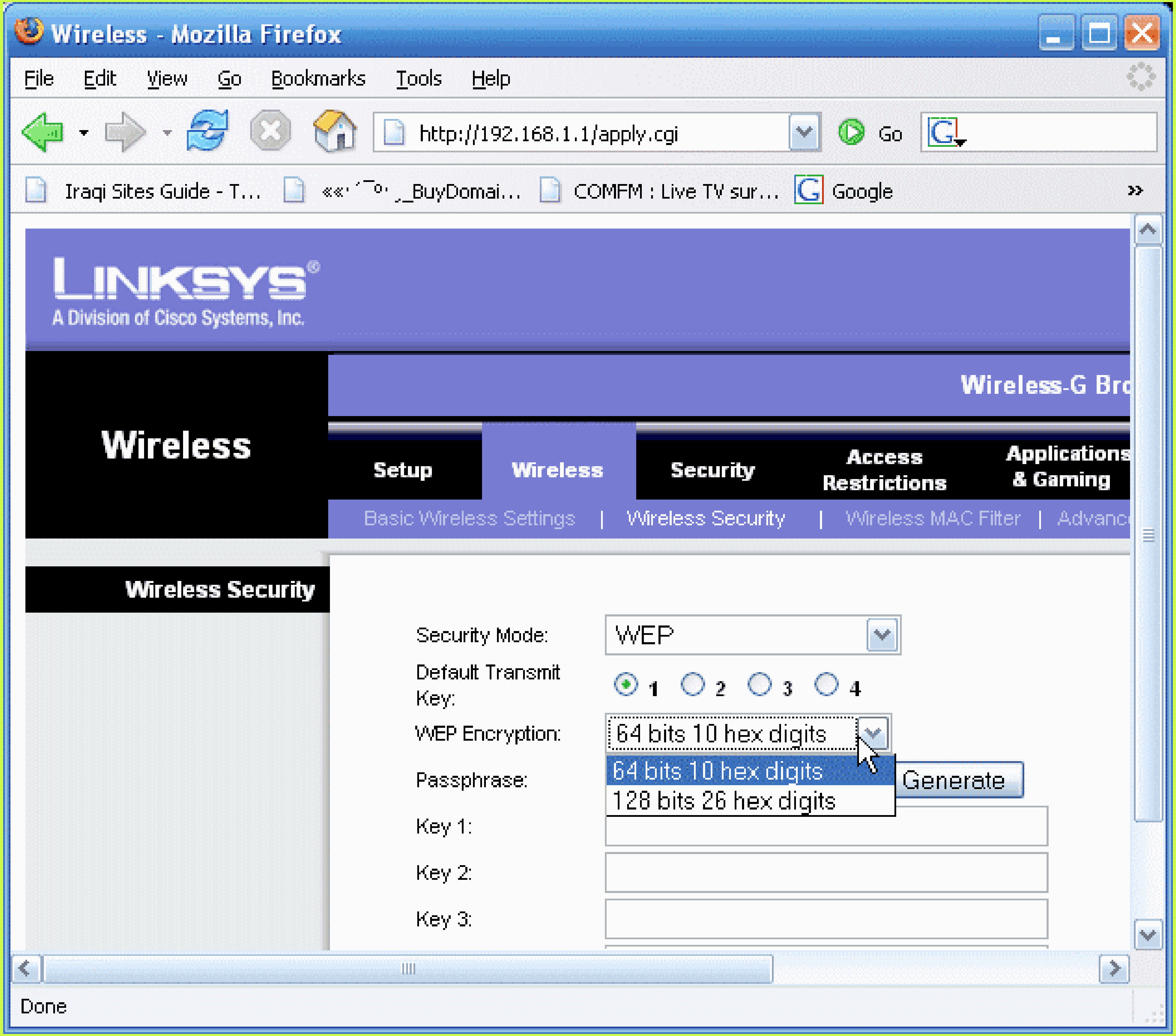


http://192.168.1.1/WL_WPATable.asp

Security Mode: Disable


Wireless - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.1.1/WL_WPATable.asp
Go
Iraqi Sites Guide - T...
«« ´ ¯ ° ´ ¸ _BuyDomai...
COMFM : Live TV sur...
Google
65.39.243.42 - Play...
»
LINKSYS®
A Division of Cisco Systems, Inc.
Wireless-G Broadband Rou
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Adminis
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Sett
Wireless Security

Security Mode: Disable



http://192.168.1.1/apply.cgi

Security Mode: WEP

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 64 bits 10 hex digits

64 bits 10 hex digits

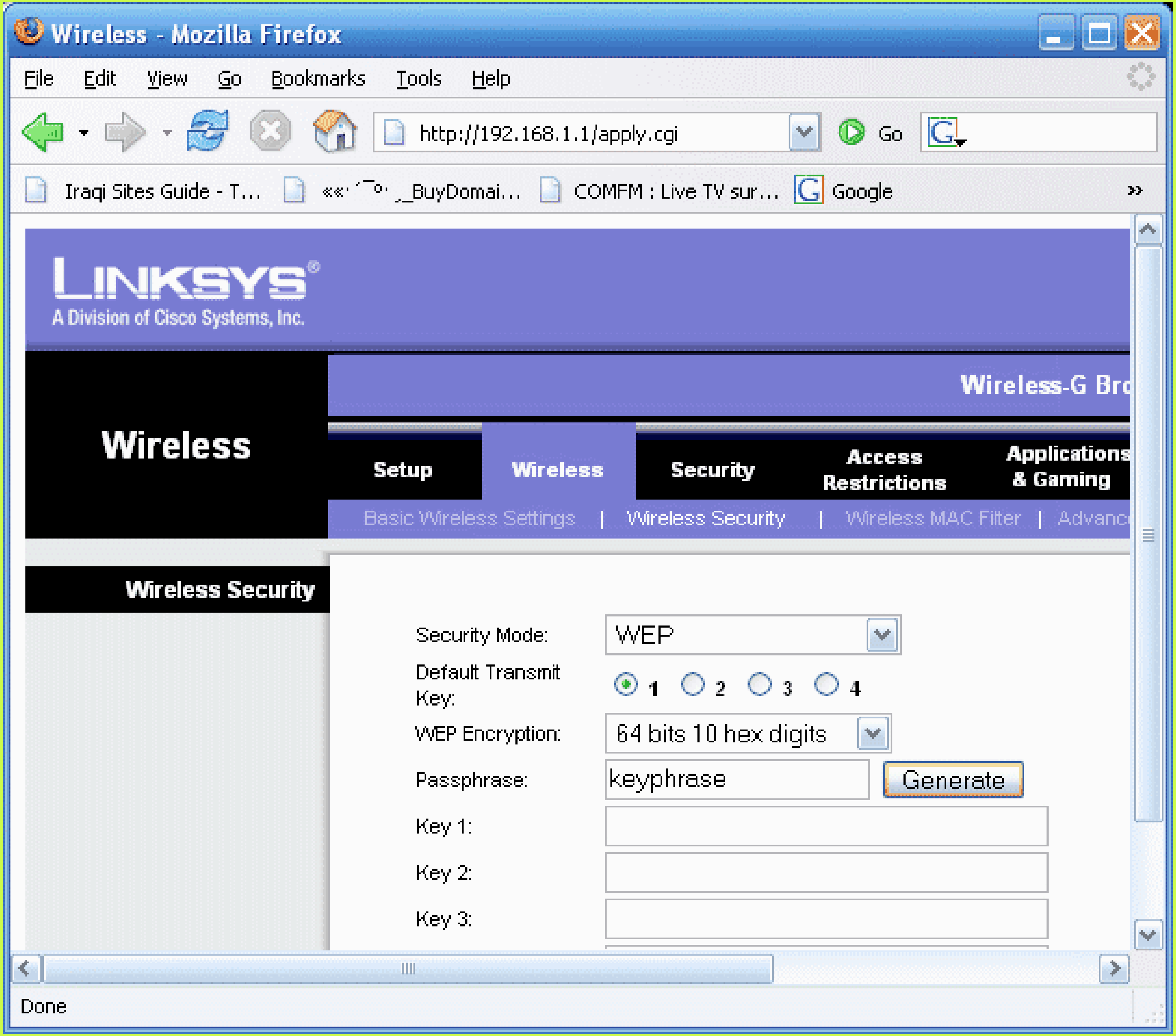
128 bits 26 hex digits

Passphrase:

Key 1:

Key 2:

Key 3:


Wireless - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.1.1/apply.cgi
Go
Iraqi Sites Guide - T...
««·´¯°·,_BuyDomai...
COMFM : Live TV sur...
Google
LINKSYS®
A Division of Cisco Systems, Inc.
Wireless-G Bro
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanc
Wireless Security
Generate
Done

Security Mode: WEP

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

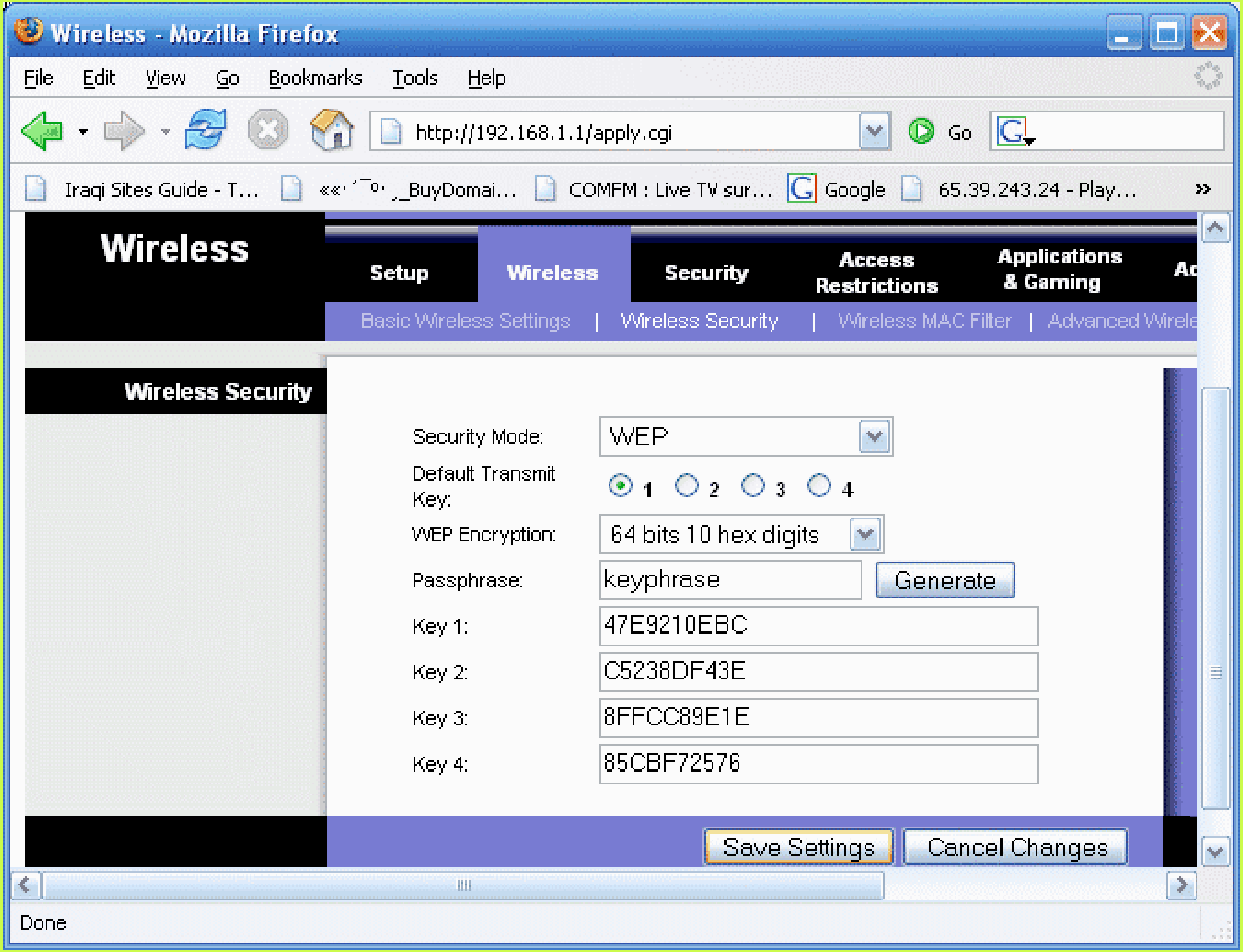
WEP Encryption: 64 bits 10 hex digits

Passphrase: keyphrase

Key 1:

Key 2:

Key 3:



Security Mode: WEP

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: keyphrase

Key 1: 47E9210EBC

Key 2: C5238DF43E

Key 3: 8FFCC89E1E

Key 4: 85CBF72576

Backup Strategy

Backup Consideration

- Document
- Label
- Verify
- Test
- Test again
- Be pessimistic

The Responsibility

- Security is **NOT** just a job function of the technical IT team; it is everybody’s responsibility.
    - Each individual is responsible.
    - Security awareness program.

The Truth

- Having the latest gizmo in place will **NOT** guarantee complete security.
- Technology and human factors have to go hand-in-hand while implementing a complete security solution.
- A security conscious and alert employee may often be able to identify, avoid or contain an incident to ensure minimal damage.

“**Information security** is a concern for everyone”