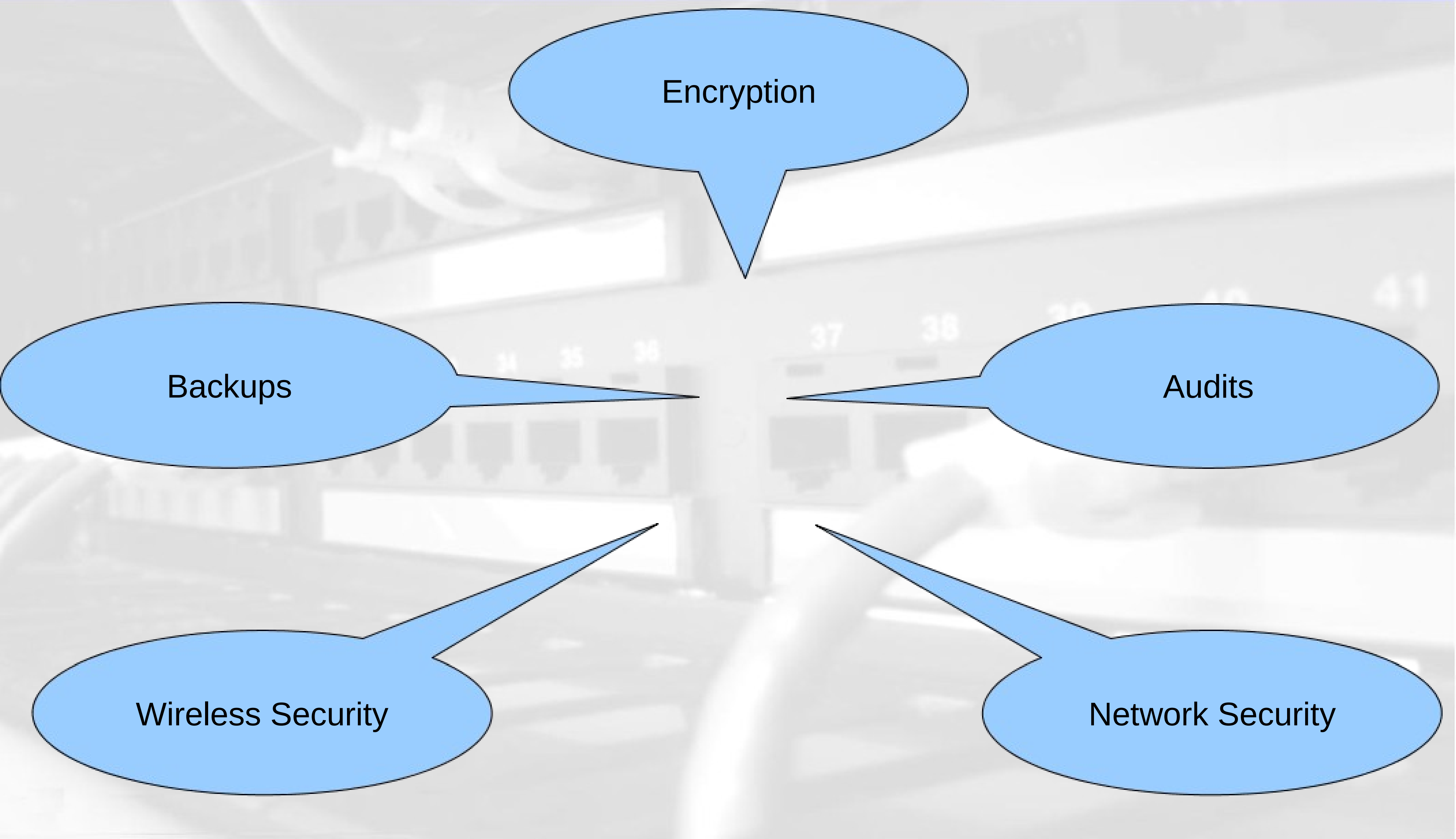
Advanced Open-Source /Free Solutions for Home and Small Business Owners

Robert Baldi, CISSP-ISSEP
Robert Clauff

TOPICS



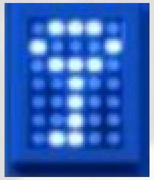
Encryption

Backups

Audits

Wireless Security

Network Security



Open Source Goodness

ENCRYPTION

- Encryption is one of the most efficient ways to secure your data
- The higher the bit rate of encryption and the algorithm depends on the quality of encryption
- When data is encrypted even if files are stolen or accessed you still need to have either a passkey or passphrase to unlock the encryption to have access to the data
- Some encryption programs that hold data can be set to destroy data with too many failed attempts at the data
- Large corporations and the U.S. government use encryption with everything to secure data
- Many encryption options without breaking the bank or a sweat

Truecrypt

- Truecrypt Portable
- Truecrypt Drive Encryption
- Truecrypt Hidden Drives

http://www.truecrypt.com

Truecrypt Local Store

- Keep an encrypted repository for sensitive files
- Once finished you may unmount for “hidden” appearance
- Can also setup to auto-mount as well
- Setup “fake” repository with different password for added security
- Very easy to use

http://www.truecrypt.com

Truecrypt Local Store Video Tutorial

http://www.truecrypt.com

Truecrypt Drive Encryption

- Great for laptops
- Encrypts entire drive for great portable data security
- Can install after OS is installed
- Can setup multiple passwords or passkeys

http://www.truecrypt.com

Truecrypt Drive Encryption

http://www.truecrypt.com

GnuPG

- Full replacement for PGP
- Supports HKP keyservers
- Fully interoperability with PGP
- Easy implementation of modules or plugins for newer algorithms
- Can be used as a filter program
- Available for Windows and Linux

http://www.gnupg.org

Tiger Envelopes

- One click install for windows or linux
- Java based application
- Secures email with encryption
- Works with Outlook, Thundbird, Kmail, and others.
- Has plugins for pgp, gpg, and bouncy castle

http://www.tigerprivacy.com

Tiger Envelopes

http://www.tigerprivacy.com

BACKUPS

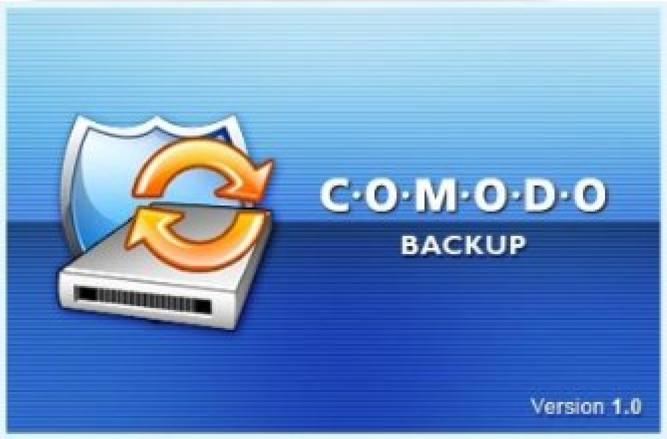
- Disaster recovery plans are a large part of security
- The location of the backups are as critical as the data you’re backing up
- SANs and NASs are often used
- If you are compromised and need to restore a server, you will be glad you have a recent backup
- Some backup software is extremely expensive
- Having a secure location and a good secure archive are good pluses to a solid backup
- Possibly having a offsite as well is a good idea as well

Comodo Backup

- Scheduled backups available
- Stores FTP, email, and other account configurations in registry with encryption
- Email alerts available for status updates
- Configure backups in minutes
- 2000, XP, and Vista support

http://backup.comodo.com/

Comodo Backup



http://backup.comodo.com/

Timevault

- Gnome based equivalent to Time Machine from Apple
- Can create incremental backups using snapshots
- Using the snapshots use a lot less space because it just uses pointers for the differences in the file

https://launchpad.net/timevault

AMANDA

- Setup a central backup server to backup to
- Backup multiple hosts to the one server
- Supports many different installations of Unix
- Uses the native dump with tar to compress the backups of multiple systems
- Easy GUI administration

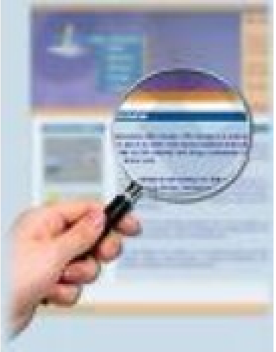
http://www.amanda.org

Openfiler

- Opensource SAN emulation application
- Vmware application or baremetal install
- Allows for SAN backups
- Cluster and high availability failover ability
- Available for use on parallels as well
- After install can be ready for use in 15minutes with fully operational SAN ability

http://www.openfiler.com

AUDITS



- Audits are great ways to monitor what is going on in your network, shares, and servers
- Audits allow you to know where your security vulnerabilities are located and what to fix
- You can audit many different things such as users and file access
- Annual or bi-annual audits on a network can keep yourself not only informed, but can maintain security
- Without audits security holes may open without your knowledge leaving vulnerabilities for malicious intent

Winaudit

- Runs inventory audit of software, hardware, network, and security settings
- Pushes reports of audits out in many different formats
- Great to get a summary of whats on a windows system

http://www.pxserver.com/WinAudit.htm

Winaudit

http://www.pxserver.com/WinAudit.htm

MBSA

- Runs a security analyzer over entire windows system
- Exports reports of all security vulnerabilities on the system in different formats
- Has 64bit support
- Can be run over selected network drives

http://www.microsoft.com/downloads/

MBSA

http://www.microsoft.com/downloads/

Open-AudIT

Open-AudIT

What's on your network ?

- Tells you exactly what is on your network
- Alerts you when any changes take place
- Information is dumped to a database for data storage
- Scheduled scans available
- Can install as a server or just stand alone application
- Windows installation coming soon

http://www.open-audit.org

DriveLook

- Index a drive for any text ever written to it
- Look over physical, logical, remote drives, and also images
- Produces tables after scan for easy access to locations
- Windows based applications

http://www.runtime.org/drivelook.htm

DriveLook

http://www.runtime.org/drivelook.htm

Truecrypt Portable

- USB drives are large security risk if containing important data with no protection
- Secure data on your portable media drives
- If you lose your USB drive, no loss of data
- Can use on full flashdrive or just a portion
- Must have admin rights to run trucrypt

http://www.truecrypt.com

Truecrypt Portable Video Tutorial

http://www.truecrypt.com

WIRELESS SECURITY

- The easiest and most acceptable into a network is from a wireless access point most of the time
- Without a very secure wireless network you will always be at risk
- Most wireless that is secured is still more than likely still at risk
- Once accessing wireless network they have full access to the internal network
- Only true way to have wireless is to have it on a separate exterior IP never touching your internal network
- Cracking wireless encryption is getting easier every day
- Not having wireless is the only true secure solution, but not realistic

Best Practices

- Always have your wireless network hidden
- Always use either WPA or WPA2
- If a radius server is available you should integrate it
- If using a personal key or passphrase and you want to be very secure use a 63 character password
- Change passwords every 3 months- 6months tops
- Implement MAC filter if possible

Kismet

- Wireless network detector, sniffer, and IDS
- Will work with any wireless card supporting rfmon
- Plugins available for more functionality
- Detects hidden networks as well

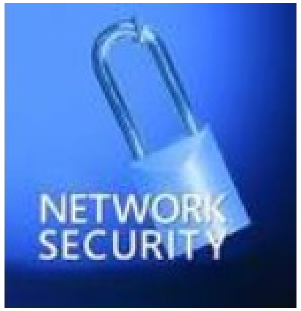
http://www.kismetwireless.net

Netstumbler

- An active sniffer for wireless access points
- Only available for Windows
- There is a mobile version for PDA called ministubler
- Doesn’t have the functionality that Kismet has

http://www.netstumbler.com

NETWORK SECURITY



- Keeping good network security is the first line of defense for your network
- Maintaining a good secure network is a huge building block for a secure environment
- Routers and firewalls at the edge of your network is one of the most important first steps
- A good firewall will deter a high percentage of malicious attempts
- However a poorly configured router will do just the opposite
- Having good applications to monitor and secure your network is a great practice to have

Nessus

- Network security vulnerability scanner
- Very configurable
- Can scan a full network of computers
- Plugins available for new signatures
- Comprises reports of every computer and their warnings and vulnerabilities
- Newest version requires corporate license, but old version still works great with updated signatures
- Version 4 is available for MAC, Linux, and Windows

http://www.nessus.org

Wireshark

- Network packet analyzer
- Great for analyzing packets inside the network
- Locking down individual incidents of network abuse
- Works great with tcpdump or windump; loading in output
- Captures can be filtered and analyzed in many different ways and several options to find the data you need

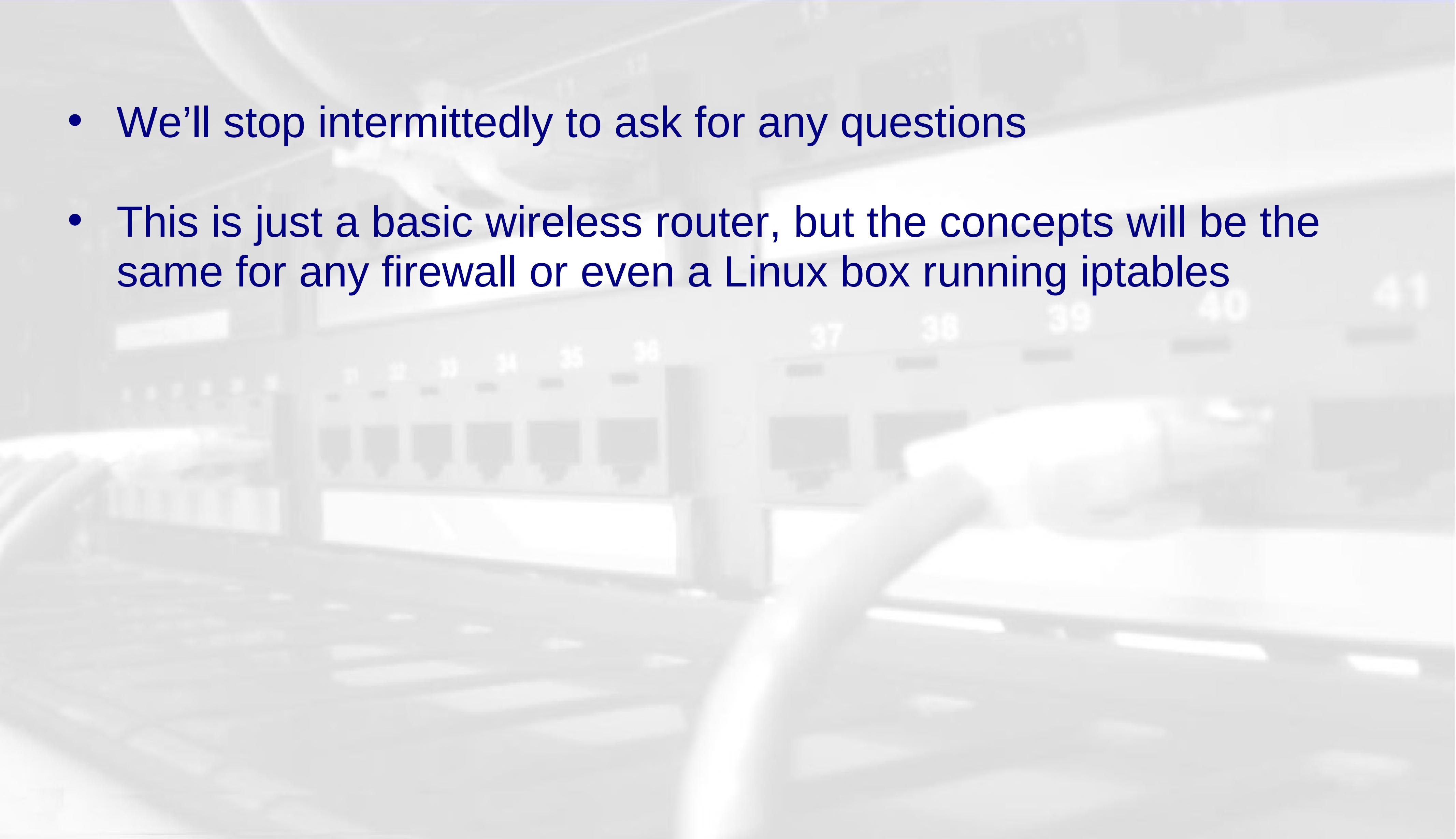
http://www.wireshark.org

Wireshark

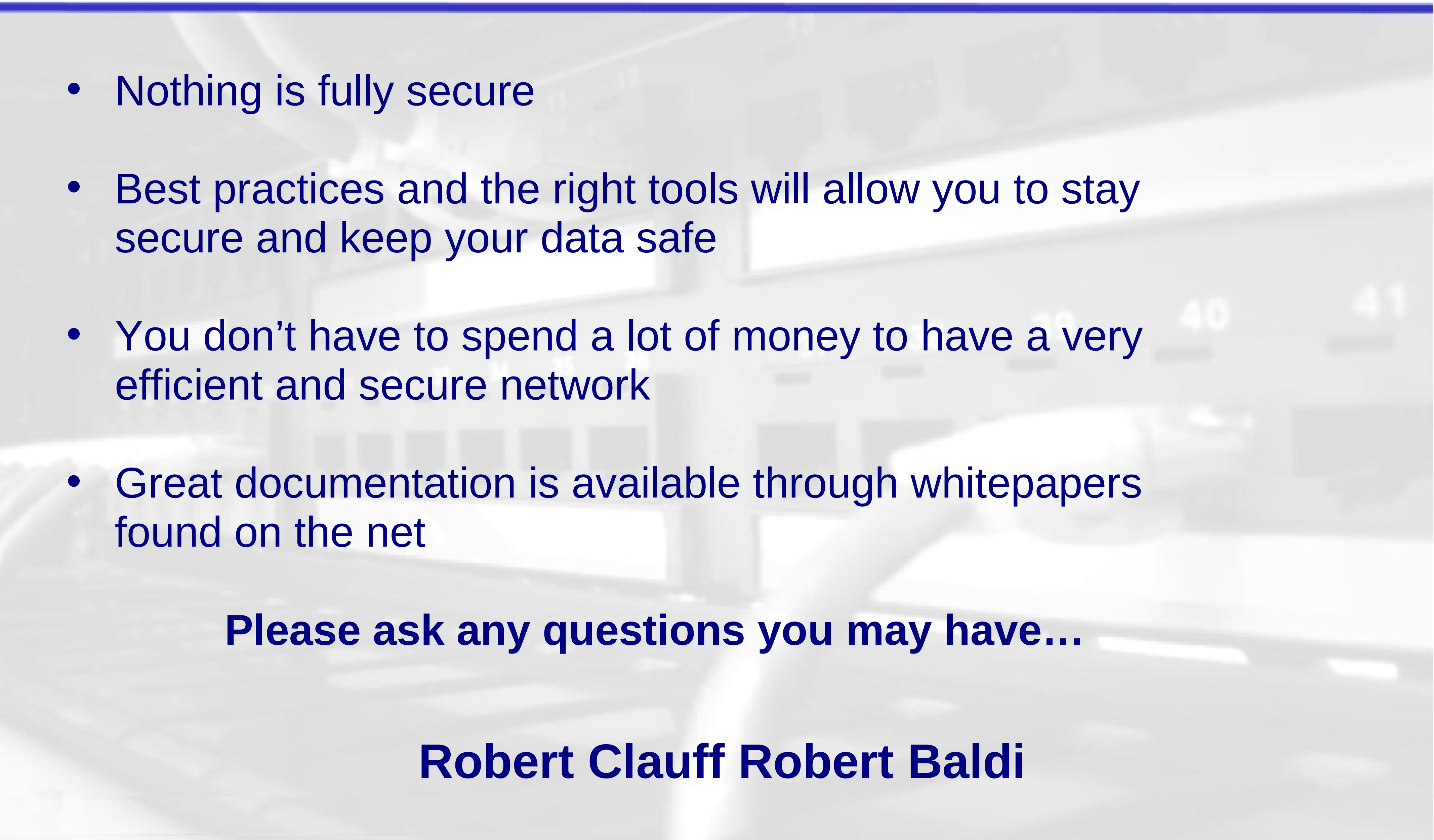
http://www.wireshark.org

Configuring a router and WiFi Live

- We’ll stop intermittedly to ask for any questions
- This is just a basic wireless router, but the concepts will be the same for any firewall or even a Linux box running iptables



Security Overview



- Nothing is fully secure
- Best practices and the right tools will allow you to stay secure and keep your data safe
- You don’t have to spend a lot of money to have a very efficient and secure network
- Great documentation is available through whitepapers found on the net

Please ask any questions you may have…

Robert Clauff Robert Baldi