

---

# DLP & Encryption

## Are They Mutually Exclusive?

---

Chris Brenton  
cbrenton@chrisbrenton.org

---

# Where Can I Get A Copy Of These Slides?

---

[www.chrisbrenton.org](http://www.chrisbrenton.org)

---

# Are They Exclusive?

---

- Encryption: Secure data so it cannot be enumerated
- DLP: Enumerate data to look for company private info leakage
- Can we fully deploy both?
  - Short answer: Sort of, but it takes a lot of work

---

# What We Will Cover

---

- Encryption
  - How it works
  - How we deploy it
  - Why it fails
- DLP
  - Host Vs. network
  - How to integrate it with encryption
- Specific recommendations

# Encryption

- Symmetrical
  - Same key to encrypt and decrypt
  - CPU efficient but key management issues
- Asymmetrical
  - Different keys to encrypt/decrypt
  - CPU heavy but fewer key management issues
  - Keys need to be larger due to mathematical relationship between them
- Both provide privacy only
  - Authentication handled through some other means

---

# Breaking Encryption

---

- Brute force the key
- Exploit the algorithm
- Exploit key management
  
- Let's talk about each in detail

# Brute Force The Key

- If at first you don't succeed; try, try, again
- Guessing speed keeps increasing
- This is why old algorithms go to pasture
  - DES excellent example
- May not be as easy as it appears
  - How do you know when you got the right key?
  - Note that challenges give up initial info
- But it can be as easy as it appears
  - Encrypted network traffic has predictable values
- Encryption should protect the data, not the session

# Exploit The Algorithm

- Considered by many to be “true cracking”
- Find a flaw which reduces the useful key space
  - We then resort to brute force
- AES as an example
  - 3 Crypto attacks release in 2009
  - None really practical...yet
  - Third reduces guesses from  $2^{256}$  to  $2^{70}$ 
    - Using 11 rounds instead of the normal 14
- Usually there is ramp up time before it's a problem

<http://eprint.iacr.org/2009/374>

# Exploit Key Management

- Typically when encryption fails, it is because key management was futzed
- WEP is an excellent example
  - RC4 used for encryption
  - RSA specs as a one time pad
    - Change keys on a per bit basis
  - Original implementation never changed keys
- Always have a “plan B”
  - RC4 was the only option with WEP
  - AES is the only option with WPA

<http://tinyurl.com/yh87p3t>

# Another Key Management Example

- Recent exploit of Kingston, SanDisk, Verbatim USB drives
- All use 256 AES to secure the drive
- All use hardware based encryption
- All certified to NIST FIPS 140-2 level 2
- All use the exact same key, all the time, regardless of the password used
- Oops!

<http://www.syss.de/>

---

# We All Fall Down

---

- Given enough time and resources, just about anything can be exploited
- 12/09 Qin Liu & Sebastien Sauge
  - Demonstrate how to man-in-the-middle Quantum Crypto as well as steal the secret key without introducing errors

<http://events.ccc.de/congress/2009/Fahrplan/events/3576.en.html>

---

# Where We Use Encryption

---

- Individual files
- Drive level
- Network

---

# File Level Encryption

---

- Used to protect an individual file
  - Both symmetric and asymmetric can be used
- Secures the data over an insecure channel
  - HTTP
  - FTP
- Masks private info from network based DLP solutions
- Can be detected by host based DLP
  - If encryption/decryption is performed on that system
  - Once secured, all bets are off

# Steganography

- The “art” of hiding information in plain sight
- Typical implementation:
  - Encrypt the file
  - Cover with a benign photo, video or sound file
  - Overlay the file onto the low order bits of the cover
- Steg as old as the Bacon Cipher (1640) still useful
  - Can appear to be poor use of elite-speak
- Not aware of any DLP solutions to catch Steg
  - Possible to view company private file in one window
  - Generate the steg file in another window

---

# Protecting Data At Rest

---

- Full disk or volume encryption
  - May need a password to boot the drive
  - May need a password to access a specific volume
- Solutions from Microsoft, TrueCrypt, PGP and others
- Protects data “at rest”
  - System powered off
  - System in sleep mode
  - Data may still be active in hibernate mode!
- Designed to protect data if laptop or drive is stolen
  - Not designed to protect active partitions

---

# Attacking Drive Encryption

---

- Key may be stored in memory
  - Usually in plain text
- Need Admin/System level access
  - Required for RAM access to key
- Cold Boot attack may be possible
  - Attacker must be quick
- These attacks only work against active data
  - Data at rest is still secured
- Host level DLP not affected by encryption
  - When checking active data

---

# File/Drive Encryption and DLP

---

- Host based relatively effective provided:
  - Encrypt/Decrypt performed on the system running the DLP agent
  - Cannot protect against sneakernet release if you let sensitive info be writing to portable drives
  - Full drive scanning performed while user is active
    - May be a performance hit

---

# IPSec

---

- Most popular VPN solution
- Outbound more of an issue than inbound
- Supports client to network, client to client and network to network
- Supports two security services, only one of which encrypts data
  - Protocol 51 (AH) usually in the clear
  - Protocol 50 (ESP) traffic is encrypted

---

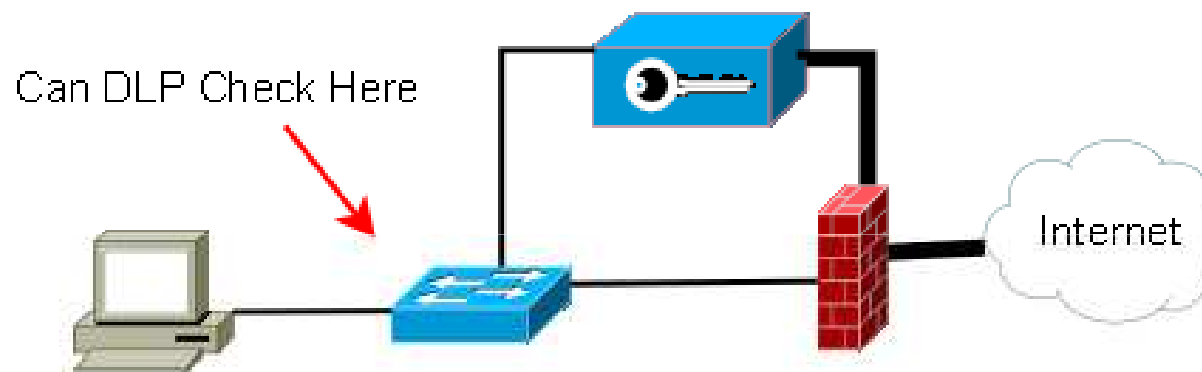
# IPSec Attacks

---

- IKECrack
  - Brute forcing tool
  - Designed to guess pre-shared secret
  - Use strong secret values or digital certificates
- FakeIKEd
  - If you know the pre-share, it can be used to grab user credentials
  - Requires ARP or DNS trickery to work

# IPSec And DLP

Client cannot generate encrypted sessions



Client can generate encrypted sessions



---

# IPSec + DLP

## Recommendations

---

- Don't let clients terminate IPSec sessions
  - Internal management OK
- Leverage your firewall
  - Block outbound protocol 50 and 51
  - From all hosts but your VPN gateway
- Or... rely on just a host based DLP

---

# SSL

---

- Client/Server based
- TLS is simply an open implementation of SSL
- Can secure any TCP based application
- A number of registered well known ports
  - HTTPS at 443 most popular
- Functionality built into every Web browser
- Can be run over any TCP port!

# SSL Attacks

- sslsniff
  - Can perform an SSL man-in-the-middle attack
  - Tools to replace auto-update files
- Clientless SSL keeps getting whacked

<http://blogs.zdnet.com/security/?p=5000>

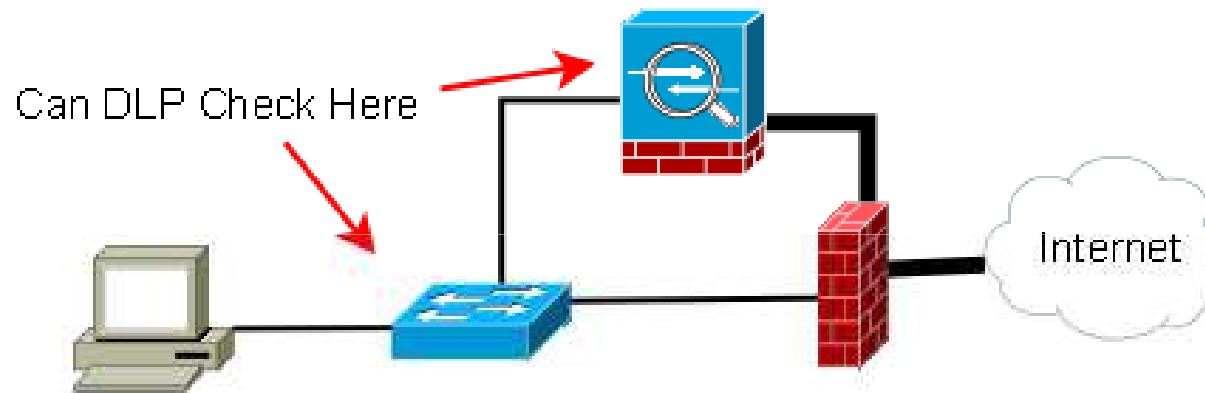
- Rogue CA's are all the rage

<http://www.phreedom.org/research/rogue-ca/>

<http://news.softpedia.com/news/Rogue-PayPal-SSL-Certificate-Available-in-the-Wild-123486.shtml>

# SSL And DLP

Client directed through an outbound proxy



Client can generate direct SSL sessions



# SSL + DLP

## Recommendations

- Force all outbound access through a proxy
  - Usually need to run non-transparent
  - Can encrypt from client to proxy, DLP check, then encrypt from proxy to server
- Leverage your firewall to limit TCP/443 access to restricted Internet sites
  - Leverage your IDS/IPS to look for SSL on non-standard ports
  - Patterns to check:
    - CipherSuite
    - SSLv{1-3} compatible client hello

---

# SSH

---

- Secure SHell
- Normally uses TCP/22
  - Can use any TCP port
- Secure replacement for Telnet & FTP
- Can be a full blown VPN
  - Can tunnel TCP based traffic
  - Can tunnel UDP with a little Netcat trickery

---

# SSH Attacks

---

- SSH protocol 1 is badly broken
  - Stick with SSHv2
- Most attacks based on brute forcing credentials
  - Can fix using public/private keys
  - Key theft can lead to further compromises
    - Don't store private keys on an active drive

---

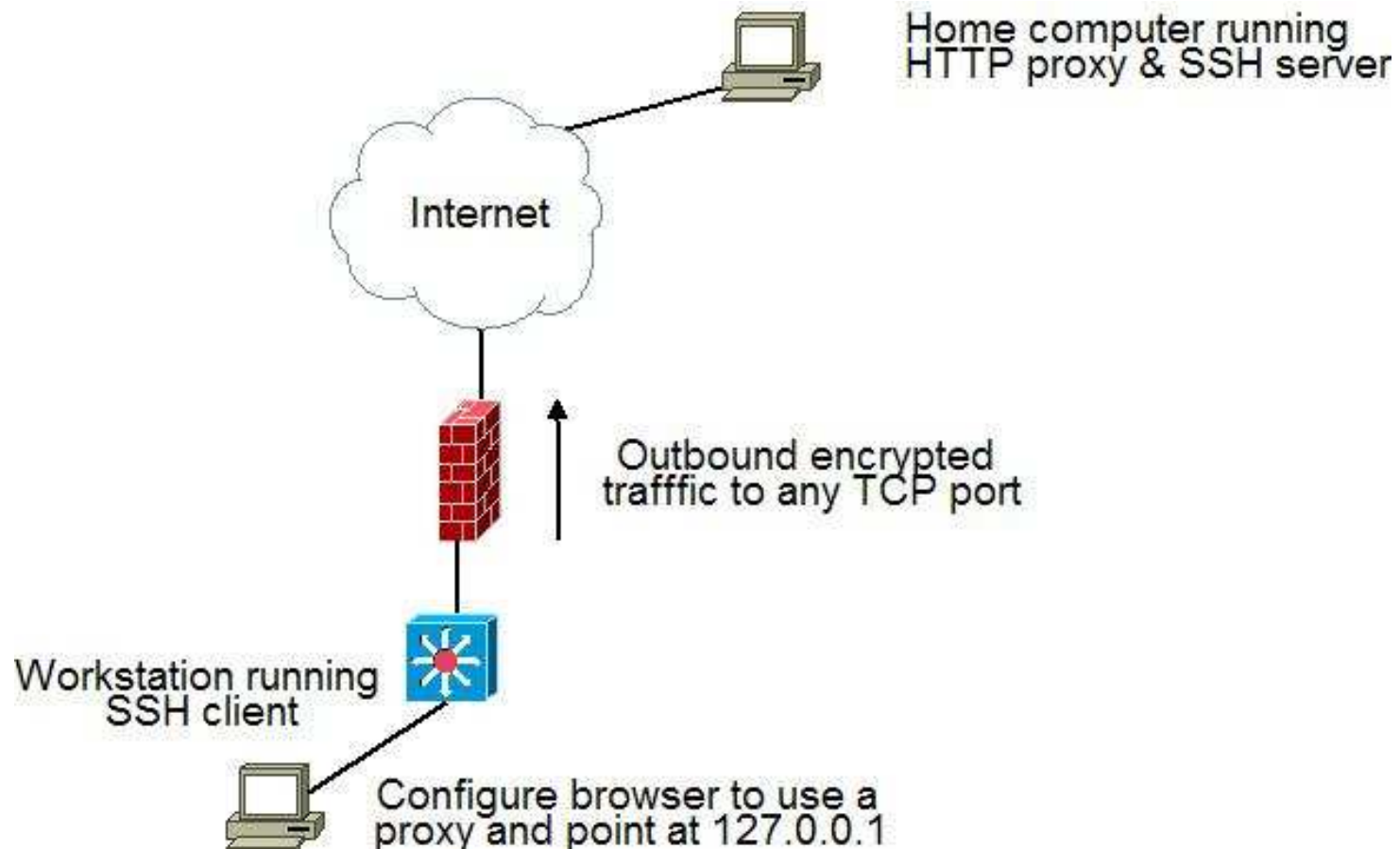
# SSH Tunnels

---

- Forward tunnels
  - Opens one or more sockets on the client system
  - Connection attempts are passed up to the server
  - Client tells the software where to send the data
    - Both remote IP and port can be specified
- Reverse tunnels
  - Opens one or more sockets on the server
  - Connection attempts are passed down to client
  - Client can forward the connection attempt to a specified IP and port

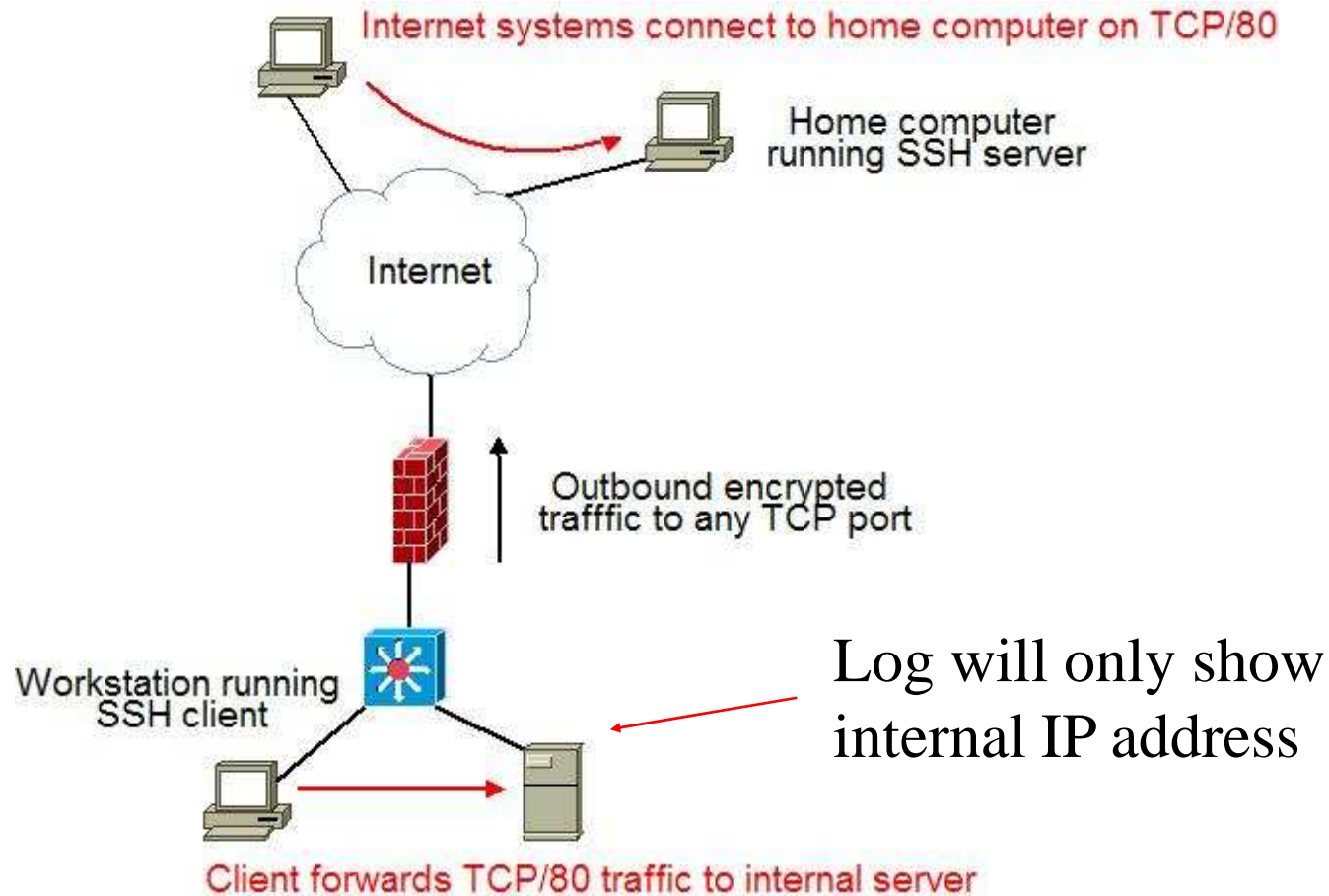
# How Does It Work?

## Forward Tunnels



# How Does It Work?

## Reverse Tunnels



---

# SSH And DLP

---

- Just say no to outbound SSH
  - Unless high trust level in the employee
  - Internal for management OK
  - Watch out for relaying
- Leverage your IDS or IPS to look for rogue traffic
  - Patterns to check:
    - SSH-1.0
    - SSH-2.0
    - diffie-hellman-group-exchange

---

# 3<sup>rd</sup> Party VPN Solutions

---

- Fine for a small shop
- Provides encrypted session to the user's desktop
  - Usually remote host based
- Provides access to data off hours
- Typically assists end users in circumventing the firewall policy
- Can be hard to spot the activity
  - Do you log outbound TCP/443? Are you sure?

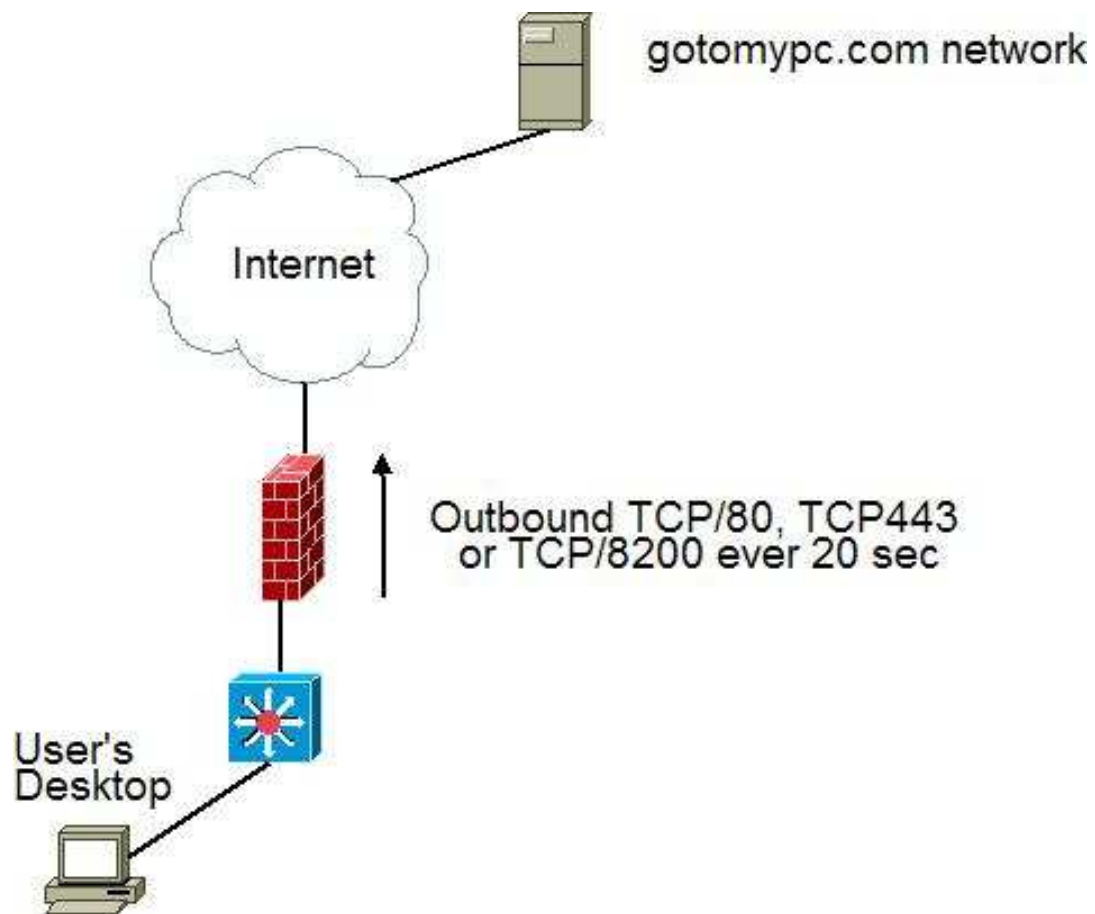
---

# Gotomypc.com – What Is It?

---

- VPN solution providing remote control of the user's desktop
- Monthly service
  - \$20/month
  - less in bulk
- Similar to MS remote access
  - Works without modification to the firewall

# How Does It Work?



---

# How To Defeat It

---

- Control the installation of software on user's desktops
  - Not always feasible
- Register with gotomypc.com to block your users
  - Must be whois listed admin contact
  - Blocks the service only
- Ban access to all gotomypc.com servers
  - 66.151.158.177/24
  
- But this just fixes this specific 3<sup>rd</sup> party solution

---

# 3<sup>rd</sup> Party VPNs and DLP

---

- Only point of opportunity is the desktop

---

# 3rd Party Server Management

---

- Common with proprietary software
  - Financial software
  - HR database
- Management is typically via VPN
  - “Required” for system management
- Problems
  - Common logon/password used on all accounts
  - If data is stolen, how can you tell?

# 3<sup>rd</sup> Party Management and DLP

- If they “own” the server a host based DLP client may not be permitted
- You are 100% committed to trusting them
  - And their employees
- Interesting stat:
  - Ponemon data breach study (PGP sponsored)
  - In 2008, 44% of data breaches caused by 3<sup>rd</sup> party partners
  - Up from 40% in 2007; 29% in 2006

<http://www.networkworld.com/news/2009/020209-data-breach.html>

---

# Summary Recommendations

## Local System

---

- Drive encryption only protects data “at rest”
  - Need other solutions while data is active
- Host based DLP is a must if end to end encryption will be support
  - You can eliminate outbound end to end encryption, but it is difficult and problematic
- If host based DLP is not used, may need some level of application control to prevent users/Malware from hiding leaks

---

# Summary Recommendations

## Network - Outbound

---

- Limit outbound encrypted tunnels as much as possible
  - Leverage your firewall
  - Leverage your IDS/IPS
- Originate outbound encrypted tunnels from your VPN gateway

---

# Summary Recommendations

## Network - Inbound

---

- Terminate inbound VPNs at your VPN gateway
- Pass in the clear behind the gateway for DLP and/or Malware checking
- Watch which security zones pass clear text traffic
- Watch out for reverse connections

---

# Summary Recommendations

## Where To Start

---

- Define security zones
- Assign numeric values
  - Based on “trust”
  - Based on data value
- Message architecture as required
- Define monitoring points between different zone values

---

# Summary Recommendations

## Where To Start (2)

---

- Sanity check your requirements
- What are your business needs for outbound encryption?
  - Buyers placing orders
  - Support monitoring/controlling clients
  - What about patches?
- What are your inbound VPN needs?

---

# How To Move Forward

---

- Only one solution for absolute security
  - And its not pretty
- Everything else is a trade off between business need Vs. security
- Assuming risk is OK
  - Provided it is a conscious and informed decision
- If your goal is absolute security, expect to hear a vortex sucking noise from your wallet

---

# Questions?

---

- Where can I get the slides?
  - [www.chrisbrenton.org](http://www.chrisbrenton.org)
- Contact info
  - [chris@chrisbrenton.org](mailto:chris@chrisbrenton.org)