



# Novel Attacks: Oblique Routes into your Network

Making Sense of Risk

Luke Jennings

8<sup>th</sup> September 2009



Who Am I?

**HACKER**





## Who Am I?





**Who Am I?**

**Security Consultant**



Who Am I?



GREY HAT



**Who Am I?**

**Penetration Tester**



# Who Am I?





## Outline

- Introduction
- Classic Perimeter Model
- Modern Reality
- Breaching the Perimeter – Client Side Attacks
- Behind the Perimeter – The Soft Chewy Centre
- Defence



## Introduction

- Many organisations highly vulnerable
- Some don't realise
- Some try to ignore the problem
- Defensive strategies often far behind offensive techniques



## Outline

- Introduction
- Classic Perimeter Model
- Modern Reality
- Breaching the Perimeter – Client Side Attacks
- Behind the Perimeter – The Soft Chewy Centre
- Defence

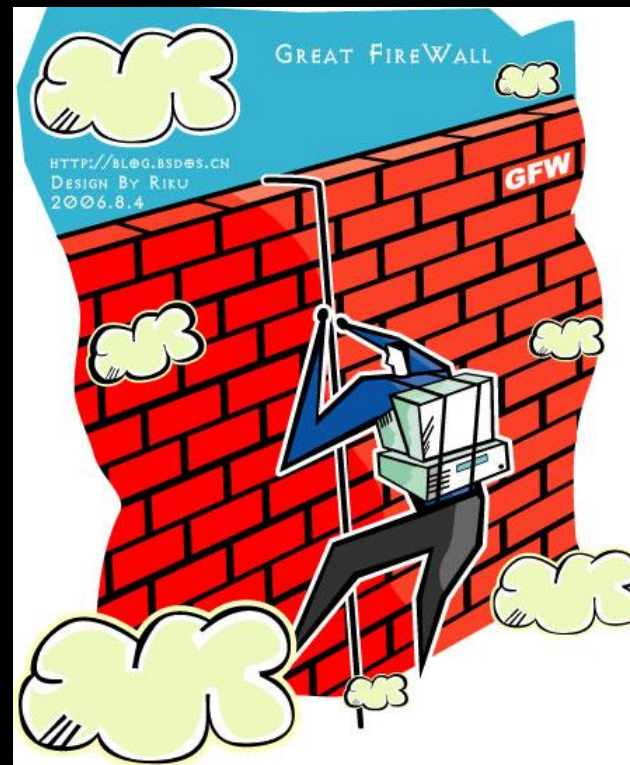


# Classic Perimeter Model



# Classic Perimeter Model - Firewalls

Outside



Inside





## Classic Perimeter Model – Problems

- Does not match modern working environment
- Personnel security not perfect
- Firewalls not insurmountable
- No defence in depth



## A Familiar Face?



## **A Familiar Face? – M&M Security**

**Kevin Mitnick**



**Once on FBI's top 10 most wanted list**

**“he could start a nuclear war by whistling into a pay phone”**

**“most organisations' security is like a hard crunchy shell with a soft chewy center - like an M&M candy”**



## Outline

- Introduction
- Classic Perimeter Model
- **Modern Reality**
- Breaching the Perimeter – Client Side Attacks
- Behind the Perimeter – The Soft Chewy Centre
- Defence



## Modern Reality

- No strict perimeter
- Third parties / contractors
- Poor physical security
- Tunnelling

## Modern Reality – Mobile Working

- Road Warriors
- Breaks your perimeter



## Modern Reality – Mobile Working

- Device theft
- Direct Attacks
- Wifi Traffic Interception





## Modern Reality – Alternate Attacks

- Firewalls prevent direct connections
- Web and email usually allowed
- Many, many possible attacks through web and email

## Modern Reality – Tunnelling

- Firewalls cause problems
- ...so everything gets tunnelled over HTTP
- ...which is allowed
- Not to mention DNS, ICMP etc





## Modern Reality – Third Parties

- Perhaps do not have same security standards as you
- ...but still get given network access

## Modern Reality – Physical Security

- Tailgating
- Believable story
- Temporary access
- Open doors / Deliveries





## Outline

- Introduction
- Classic Perimeter Model
- Modern Reality
- Breaching the Perimeter – Client Side Attacks
- Behind the Perimeter – The Soft Chewy Centre
- Defence



## Client Side Attacks – Why?

- Conventional attacks
  - Small surface area
  - Hardened builds
  - DMZs



## Client Side Attacks – Why?

- Client Side Attacks
  - HUGE surface area
  - No DMZ
  - Many 0-days
  - Bad patching
  - AV difficult
  - Clever Payloads



## Client Side Attacks – Surface Area

- Web
  - HTML parsing is complex
  - ...so is JavaScript
  - Many multimedia formats
- Email
  - Can deliver any file type
  - PDFs, Office docs, JPEGs etc

## Client Side Attacks – Impact

- No DMZ
- What if it hits your admins?
- VPN-like tunnels
- Proxy and Host Firewall bypass





## Client Side Attacks – Vulnerability

- Lots more to patch
- WSUS isn't enough
- 0-days are common
- Some exploits can't be "patched"
  - Do you use word macros?

## Client Side Attacks – Detection

- Anti-virus is tricky
- Lots of input vectors
- Custom encodings
- Often easy to beat (PEScrambler)





## Client Side Attacks – Real World

- 80% run vulnerable Adobe Flash
- 83.5% run vulnerable Adobe Reader
- In April 2007 researchers at Google discovered hundreds of thousands of web pages performing drive-by downloads.



## Client Side Attacks – Demos

- Web based attack
- Malicious Attachment



## Outline

- Introduction
- Classic Perimeter Model
- Modern Reality
- Breaching the Perimeter – Client Side Attacks
- Behind the Perimeter – The Soft Chewy Centre
- Defence

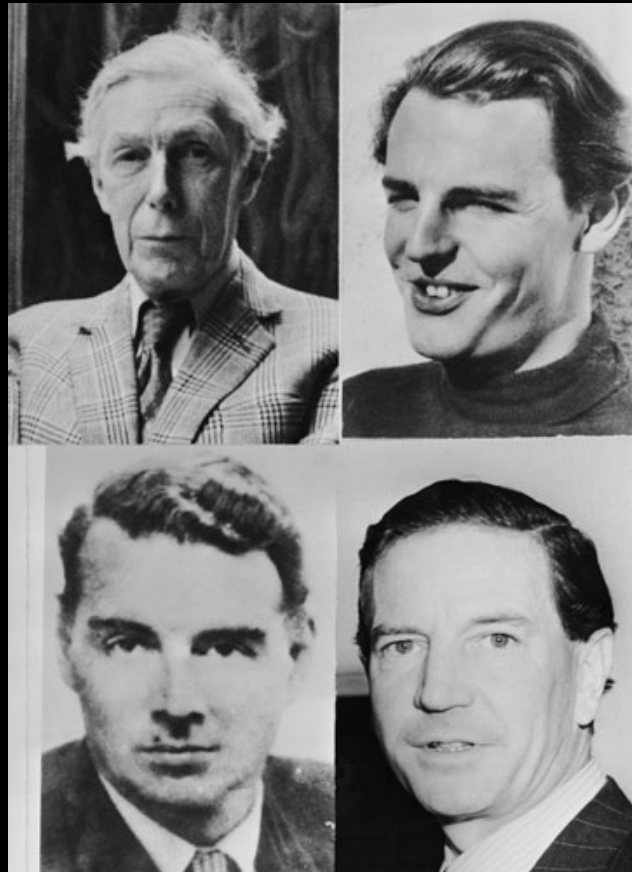
## Internal Attacks – The Threats

- Hackers Circumventing Firewall
- Physical Intruders
- Insiders





# Internal Attacks – Insiders





## Internal Attacks – Open Environment

- Little or no internal filtering
- Weak internal physical security
- Slow adoption of NAC
- ...easily defeated when implemented



## Internal Attacks – System (Mis-)Management

- Weak Passwords
- Shared passwords
- Unpatched systems
- Powerful service accounts



## Internal Attacks – My Experience

- Clear text services are my friend (but not yours)
- Service accounts often neglect password policy
- I always get Domain Admin



## Internal Attacks – My Experience

- Clear text services are my friend (but not yours)
- Service accounts often neglect password policy
- I always get Domain Admin



## Outline

- Introduction
- Classic Perimeter Model
- Modern Reality
- Breaching the Perimeter – Client Side Attacks
- Behind the Perimeter – The Soft Chewy Centre
- Defence



## Strategic Defence

- Support modern business working practices securely
- Reduce risk from internal threat agents
- Maintain a current security awareness

## Tactical Defence

- Ensure patch management addresses desktops adequately
- Use disk encryption to protect mobile workers
- Segregate internal network
- Staff vetting





## Operational Defence

- Client Side Penetration Testing
- Internal Penetration Testing
- Physical Security Testing
- Desktop and Laptop Security Reviews



Questions?

