VPNs: Security's Magic Bullet

James Eaton-Lee

Licensing

Abstract / Introduction

- Virtual Private Networks (VPNs) are a networking tool widely used to increase the security of IT systems.
- A VPN is a powerful tool, but is often used inappropriately.
- Many VPN implementations actually reduce overall security.
- VPNs, intended to protect against external threat, increase exposure to internal threat - yet internal threat is usually the greatest risk to an organisation.
- We will examine what VPNs are for, what high-level problems anyone securing them faces, and some specific flaws in VPNs.
- We will examine ways of remediating or avoiding these problems.

What is a VPN?

- VPNs are designed to solve one problem effectively: *seamlessly linking physically separate hosts and networks*. Everything else VPNs do is related to this goal, or a special case of it.

- The term VPN, much like the term Voice over IP (VoIP) is a blanket term referring not to a specific piece of technology, but a category of pieces of technology, all designed to work in similar ways and solve similar problems.

What security is, and why it matters.

- All too frequently, security is not given proper consideration – it is over, or under, emphasised. Finding the right level of security for your environment is of paramount importance!

- Many principles of security are also principles adhered to by *reliable*, *scalable* systems; if we build a system which is secure, it will probably meet our other needs better too.

- The CIA Triad:
  - Confidentiality – ensuring the privacy of our data and systems; making sure only we have access to them.
  - Integrity – ensuring the state of our data (and systems), and making sure they aren’t modified by anyone unauthorised to do so.
  - Availability – ensuring that we have access to our data and systems when we need them.

Some Statistics..

Roughly 36% of UK businesses allow some staff to access their systems from a remote location (e.g. from home or via wireless hotspots). Four-fifths of large businesses allow this.

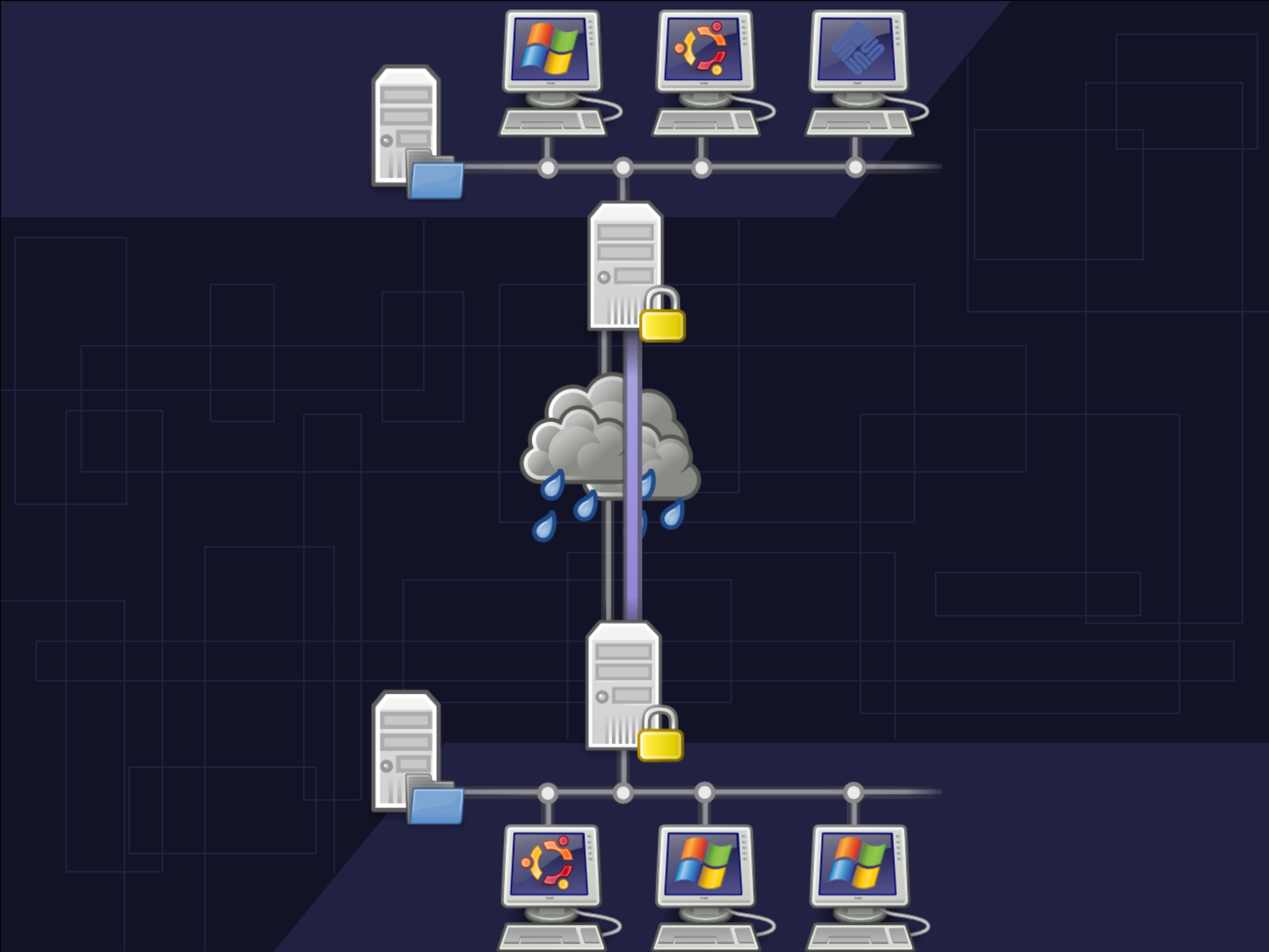
Interestingly, respondents who allow remote access are twice as likely to have had an unauthorised outsider try to break into their network as those who do not; they are also more likely to have experienced an actual penetration incident.

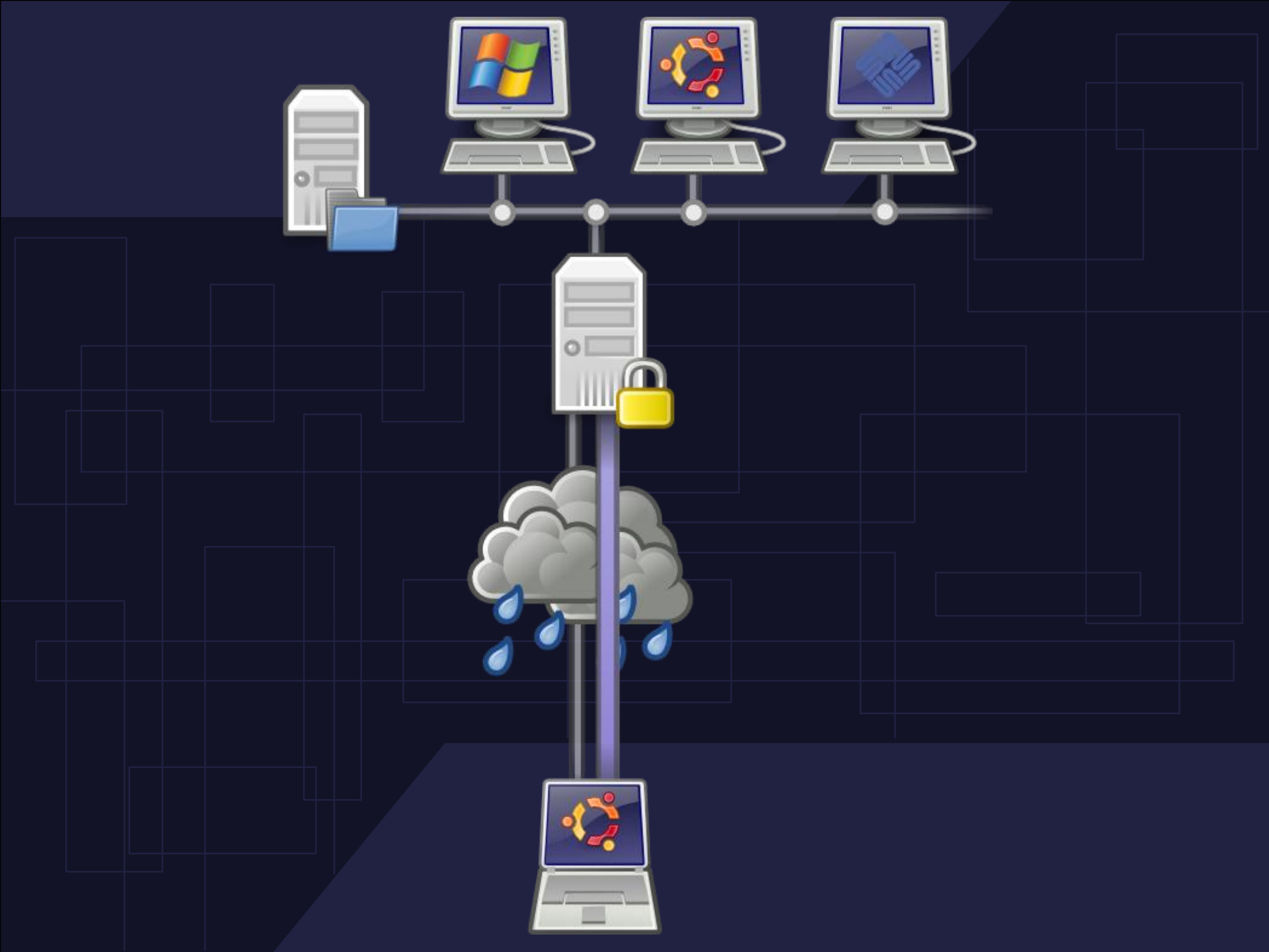
The overwhelming majority (94%) of companies allowing remote access restrict either the staff who can do this or the systems they can access remotely. Those that do not are twice as likely to have had an outsider actually penetrate their network.

- PWC/DTI Information security breaches survey 2006 (emphasis mine)

How VPNs are used.

- Site-to-Site VPNs
- Roadwarrior VPNs
- Protecting Wireless Networks
- Accessing a secure DMZ





General VPN Problems

1. Username Enumeration

No-one who isn't allowed access to our systems should be able to find out who is.

"To login successfully on the UNIX system, it is necessary after dialling in to type a valid user name, and then the correct password for that user name. It is poor design to write the login command in such a way that it tells an interloper when he has typed in a invalid user name. The response to an invalid name should be identical to that for a valid name.

When the slow encryption algorithm was first implemented, the encryption was done only if the user name was valid, because other-wise there was no encrypted password to compare with the supplied password. The result was that the response was delayed by about one half second if the name was valid, but was immediate if invalid. The bad guy could find out whether a particular user name was valid. The routine was modified to do the encryption in either case."

Password Security: A Case History (1979), Robert Morris & Ken Thompson

General VPN Problems

2. Account Lockout

Unauthorised users should not be able to prevent authorised users from logging in.

"In an account lockout attack, the attacker attempts to lockout all user accounts, typically by failing login more times than the threshold defined by the authentication system. For example, if users are locked out of their accounts after three failed login attempts, an attacker can lock out their account for them simply by failing login three times.

This attack can result in a large scale denial of service attack if all user accounts are locked out, especially if the amount of work required to reset the accounts is significant"

Open Web Application Security Project (OWASP) Wiki

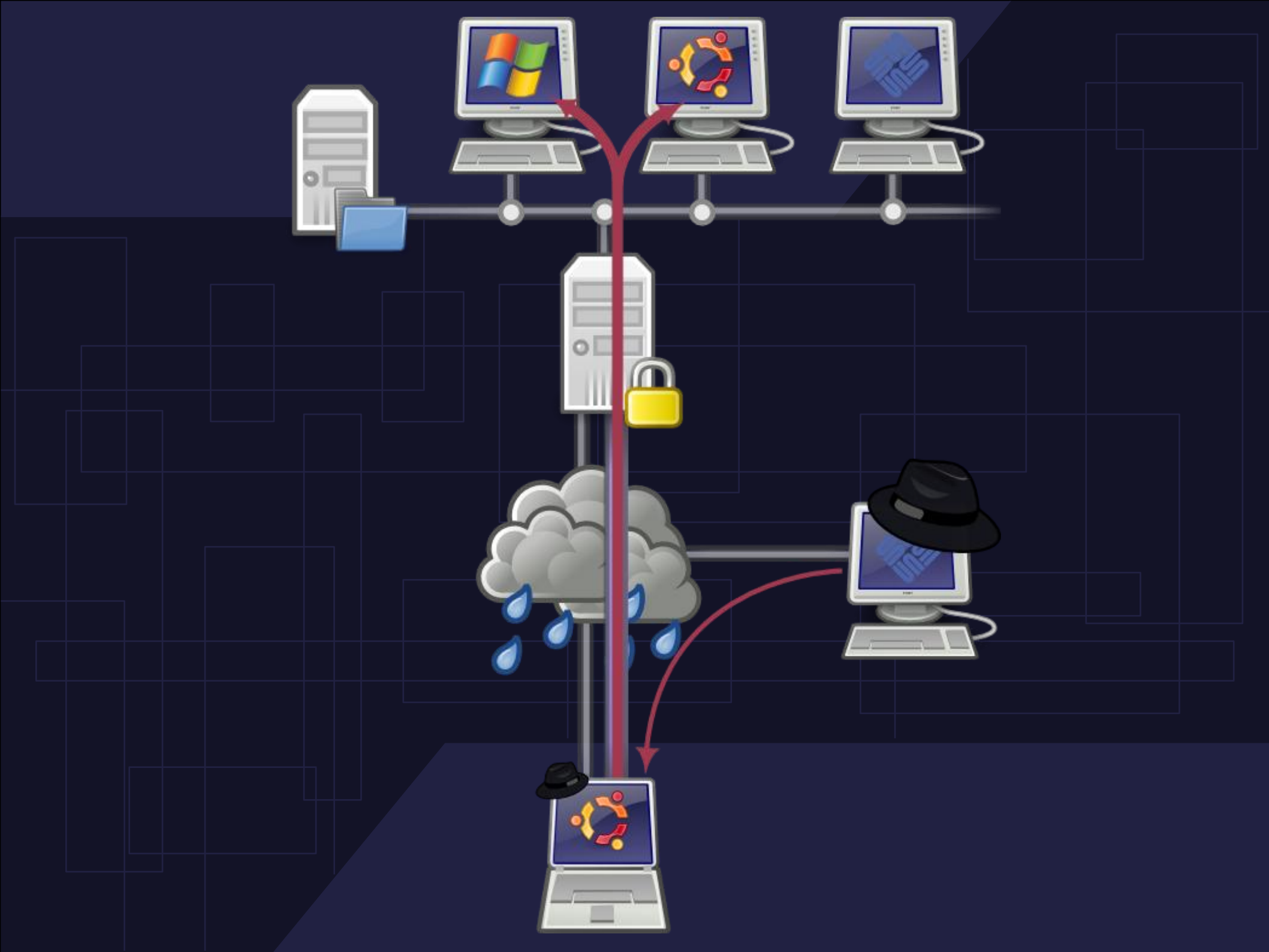
http://www.owasp.org/index.php/Account_lockout_attack

General VPN Problems

3. Lack of Proper Firewalling

Authorised users should only be able to access resources they're authorised to use.

- VPNs grant internal users access to internal resources in a similar manner to other LAN clients – by essentially turning a remote client into a local LAN client.
- Remote clients are subject to an extra avenue of attack local clients are not susceptible to – direct attack from users on the internet and the network they're connecting from (such as a wireless network or hotel network).
- If a remote client is compromised, the resulting is similar to that of a rogue wireless access point or malicious intruder within the LAN environment.
- Any attacker who compromises a remote client with total access to our internal network, has total access to our internal network.
- Within the context of site-to-site VPNs, inadequately firewalling makes insider threats and viruses / worms a far larger threat.



VPN Security Problems

Architectural problems

- Account Lockout
- Username Enumeration
- Lack of Proper Firewalling
- Split Tunnelling
- Difficulty of Auditing VPN Traffic

(Some) Protocol-Specific problems

- Client Software Weaknesses
- Problems with IKE
- Certificate Authentication Issues
- Kerberos Authentication Issues

Architectural - Account Lockout

Problems

- Attackers can attempt to authenticate many times.
- Most networks configure policies designed to present brute-forcing of accounts involving an account lockout after *N* unsuccessful authentication attempts
- These policies can be used to deny legitimate users access to the VPN and potentially other systems too.

Potential Resolutions

- Review lockout policies.
- Throttle login attempts at the VPN Endpoint.
- Configure stricter backoffs at the VPN endpoint than the lockout policy itself.
- Adequately configure Authentication Mechanism (Radius, AD, eDirectory, etc)
- Highly implementation-specific

Architectural - Account Enumeration

Problems

- Attackers can attempt to authenticate using arbitary usernames.
- The response given by the VPN Endpoint to an authentication attempt utilising a *valid* username, and one utilising an *invalid* username, can differ.
- This difference can be manipulated to generate a list of valid usernames.

Potential Resolutions

- Use a VPN Implementation that does not have this problem.

Architectural - Lack of Proper Firewalling

Problems

- Once authenticated, users have access to all network resources.
- We rely very heavily on the authentication process for security.
- Users don’t look after their authentication details (passwords, tokens, etc.)
- VPN Clients can be attacked in ways unique to them.

Potential Resolutions.

- Solve the User Problem.
- Very heavily lockdown client machines.
- Identify what requirements users have, and restrict their traffic so that it meets these requirements and no more.

Architectural - Split Tunnelling

Problems

- Using a '*default route*' via the VPN tunnel, all traffic, including web traffic, traverses the VPN.
- This is slow. Users and admins dislike it. It is frequently bypassed.
- Bypassing exposes a machine to attack from the entire internet, whilst being connected to the corporate LAN.

Potential Resolutions

- Clear, enforced IT/Security Policies regarding clients and VPNs.
- Totally lockdown Clients and configure them properly.
- Break routing in such a way as to make it harder to configure clients this way.

Architectural – VPN Auditing

Problems

- Logs aren't easy to audit.
- Auditing is time-consuming.
- Admins are (lazy|overworked)
- How do you define legitimate and illegitimate access?
- Most VPN Endpoints offer very sparse functionality in this respect.
- Not many (especially SOHO devices) allow you to monitor, or filter, Network Traffic.

Potential Resolutions.

- Solve Admin Problems / increase awareness.
- Use Log Analysis tools and scripts.
- Upgrade your VPN Platform.
- Use an authentication mechanism such as RADIUS designed for central accounting and log analysis.
- Routinely monitor VPN Network Traffic itself.

Protocol or Software Specific – Client Weaknesses

Problems

- Storage of Credentials
- Man in the Middle Attacks
- Users are frequently able to setup VPN Connectoids on arbitrary machines.

Potential Resolutions

- Clear, enforced IT/Security Policies regarding clients and VPNs.
- Totally lockdown clients and configure them properly.
- Negate users' ability to configure their own VPN Connectoids, eg. Using non-exportable certificates.
- Use high-quality Software.
- Keep this software up to date.

Protocol or Software Specific - IKE

Problems

- IKE is a complicated protocol, and part of a suite of similarly complicated protocols.
- Unfortunately, some parts of the IKE Specification aren’t specific enough.
- IKE implementations vary. This variation can be manipulated.
- Username Enumeration via IKE.
- UDP Backoff Fingerprinting.

Potential Resolutions

- Use a decent IKE implementation.
- Understand what your IKE implementation allows attackers to do and find out.
- Decide whether or not you’re comfortable with this.
- Don’t use IKE.

Protocol or Software Specific - Certificates

Problems

- X.509 certificates are a widely used (semi-)standard for storing information.
- Some of this information may be used to secure VPN or SSL Connections.
- Attackers can see bits of the information that don’t need to be used as part of the security process - in the *Certificate Request Payload*

Potential Resolutions

- Understand what your use of certificates allows your attackers to find out.
- Configure your IKE/IPSec implementation properly; use an implementation that can withhold CA data from the CRP.

Fixing VPN Problems - *Remediation*

- Is highly variable from implementation to implementation.
- Requires that you first identify your needs, and then ensure that your VPN is meeting only those needs and any more.
- May require a degree of accepted risk – a common firewall policy across VPN clients, for instance.
- Is sometimes disruptive and painful, as well as complex and time-consuming to manage – don’t overcomplicate things.

Alternatives to VPNs

- Deliver services directly via the web.
- Several benefits to delivering services to users via http(s), namely:
  - We have a solution tailored to our business goals
  - We can deliver significantly better service & support
  - We can avoid firewall and mobility issues
  - Generally more cross-platform

- Some security observations re: this approach:
  - Any attacker who acquires credentials to a web service can only attack specifically that web service
  - Web services are frequently designed for internet exposure
  - There are a wide range of security mechanisms we can leverage
    - Certificate-based authentication
    - HTTP(s)
    - Application-layer firewalling (this is really cool)
    - Ease of segregation from the network infrastructure

- What I am not saying
  - Just expose all your services to the internet
  - This is a viable total replacement for VPNs you can implement tomorrow
  - VPNs should die
- What I am saying
  - A large number of VPN users access a small subset of services, such as E-Mail, File Access, business-related applications , access databases, etc
  - Many of these services are very easy to deliver via the web

- E-Mail / Groupware
  - A wide range of web-based products for these.
  - IMAP access – also securable via ssl & auth
  - MS Exchange – RPC over HTTP, OWA
- File Access
  - Webdav! Webdav is great.
  - Web-based document management
- Business applications
  - Often have web-based cousins, e.g. Web-based ACT!
  - Can often be transitioned to intranet environments.

Conclusions

- *"With great power comes great responsibility"* - Spiderman (Peter Parker)
- If you’re considering just dropping in a VPN as an interim solution, please think carefully about it.
- There’s no such thing as an interim solution.
- Whichever strategy, we should be deliberate about it and ensure that it aligns with what our goals ultimately are.