The University of Auckland
NEW ZEALAND

Handling spam and malware (IT Tertiary Conference 2004)

Russell Fulton

<r.fulton@auckland.ac.nz>

Bojan Zdrnja

<b.zdrnja@auckland.ac.nz>

Overview

- Introduction
- UoA e-mail system – Bojan
- Coping with non e-mail threats – Russell
  - **Protecting hosts & detecting infections**
- Questions

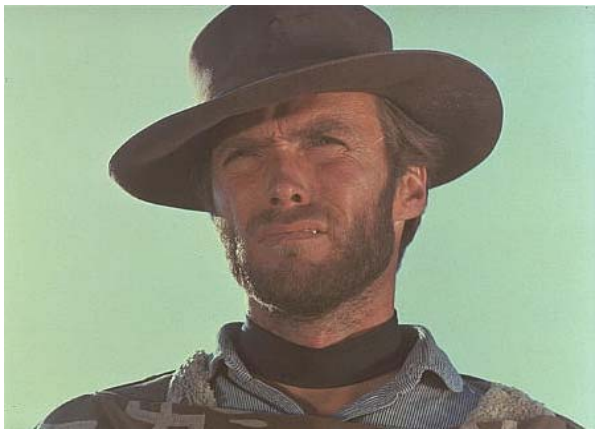
What we have to deal with (the bad side)

- Number of viruses/worms is rising
  - **Over 100.000 new malware in 2003 – this makes 200 per week**
  - **Only a small part gets ItW (In the wild)**
  - **Most are zoo collections**
- Malicious software causes huge damage
- At least 60% of all e-mail is spam

What we have to deal with (the ugly side)

- Users demand “instant” e-mail
  - **Although e-mail was never intended to be instant**
- Users want to send their files easily
  - **Which enables malware to do the same**
- Users don’t want any spam in their mailboxes

What are our goals? (the good side)



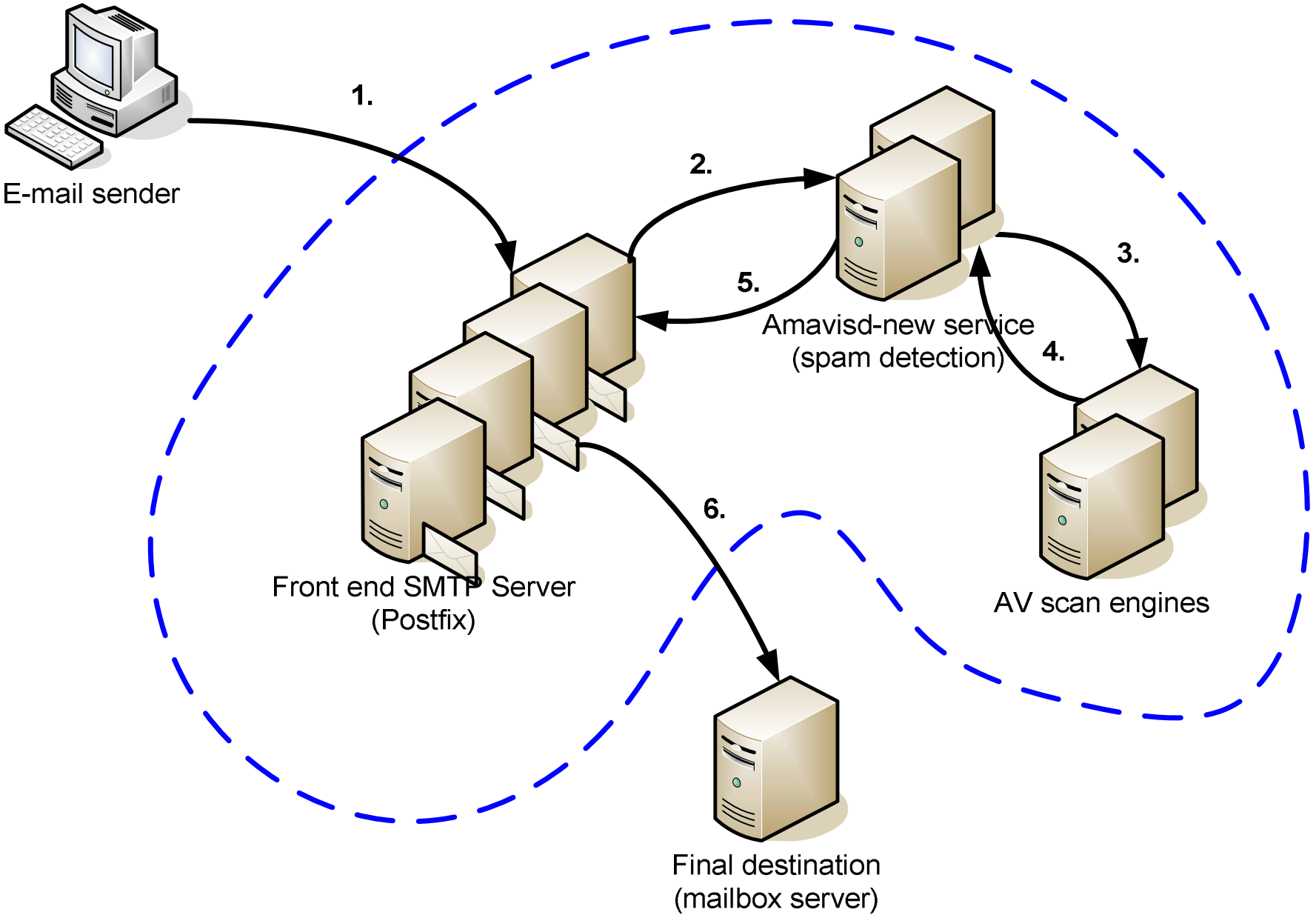
- E-mail system has to be reliable
- Robust with redundancy
- Scalable
- As always in security: multiple layers for everything

Our requirements

- ~6,000 staff, ~40,000 students
- ~15,000 class lists, ~10,000 mailing lists
- Does it really matter?
- Not really, because:
  - **6,000 staff deal with 200,000+ e-mails daily**
  - **40,000 students deal with 50,000+ e-mails daily**

Current UoA e-mail system

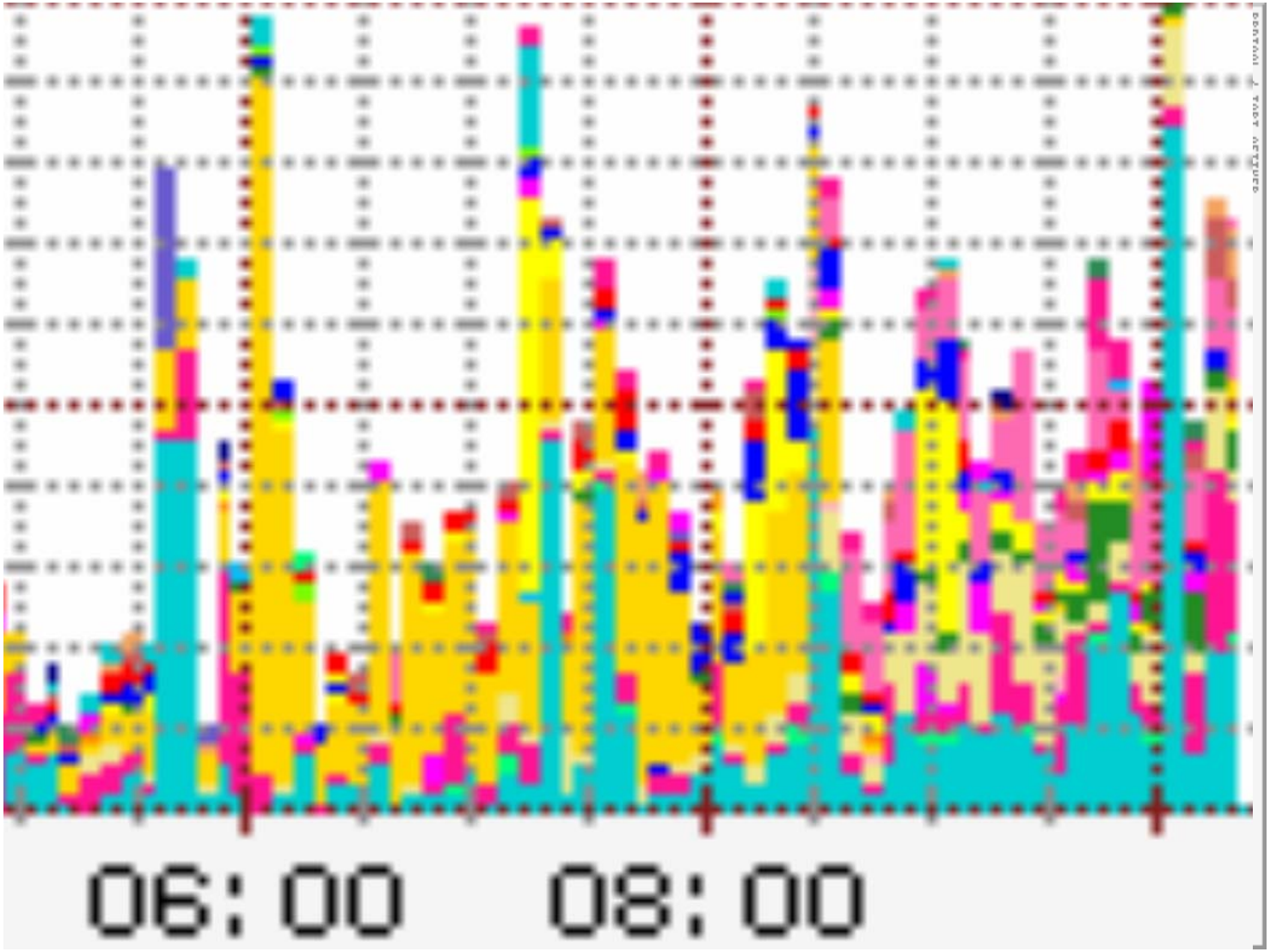
- Completely redundant, cluster of 4 servers
- Extremely scalable
  - **Easy adding of new servers to increase throughput**
  - **Possible separation of services**
- Multiple AV scanning engines
- Multiple anti-spam engines


E-mail sender
1.
2.
3.
4.
5.
6.
Amavisd-new service
(spam detection)
Front end SMTP Server
(Postfix)
AV scan engines
Final destination
(mailbox server)

AV detection and policy

- Our policy:
  - **Drop infected messages (*NO* notifications)**
  - **Quarantine all executables (recipient notified)**
- How to detect banned attachments?
  - **By extension**
  - **By file type**
  - **By content**
- How deep will we inspect?

Blocking executables

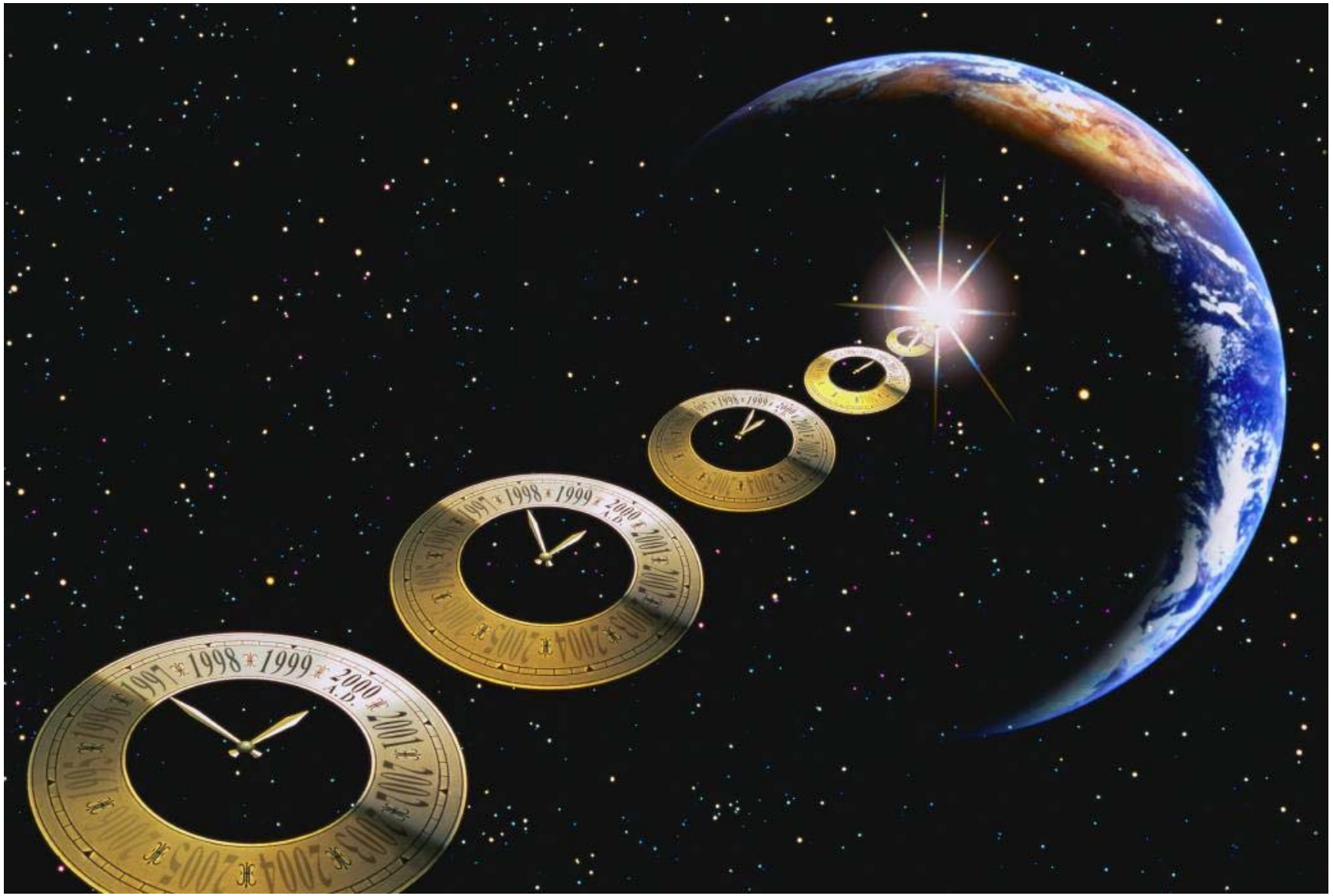


AV detection and policy

- Detection by extension
  - **Simple to implement, easy to evade**
- Detection by file type
  - **Used currently**
  - **File type decided by the “magic header”**
  - **Uses ‘file’ utility**
- Detection by content
  - **Very difficult**
  - **JavaScript in HTML**
  - **Macros in Word & PDF documents**

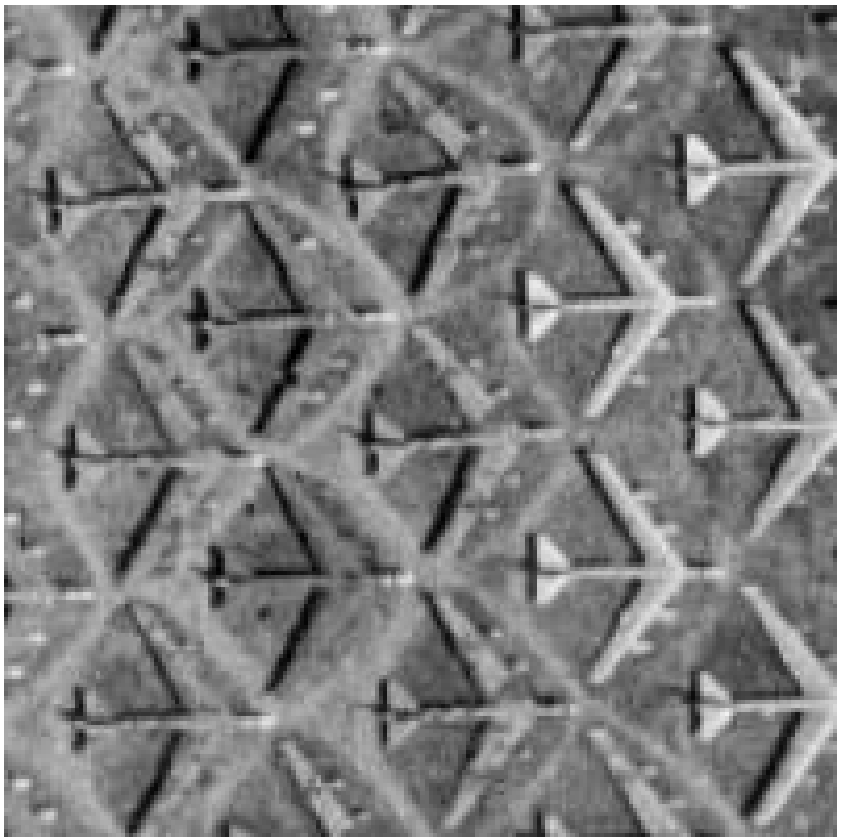
AV detection and policy

- No e-mail filter can stop a determined user
- Couple of possibilities
  - **Change file type (hexedit)**
  - **Use “strange” file types (different parsing)**
  - **Use cryptography**
- Steganography
  - **Files through images**
  - **Files through audio files**
  - **http://www.petitcolas.net/fabien/steganography/**


1998
1999
2000
A.D.

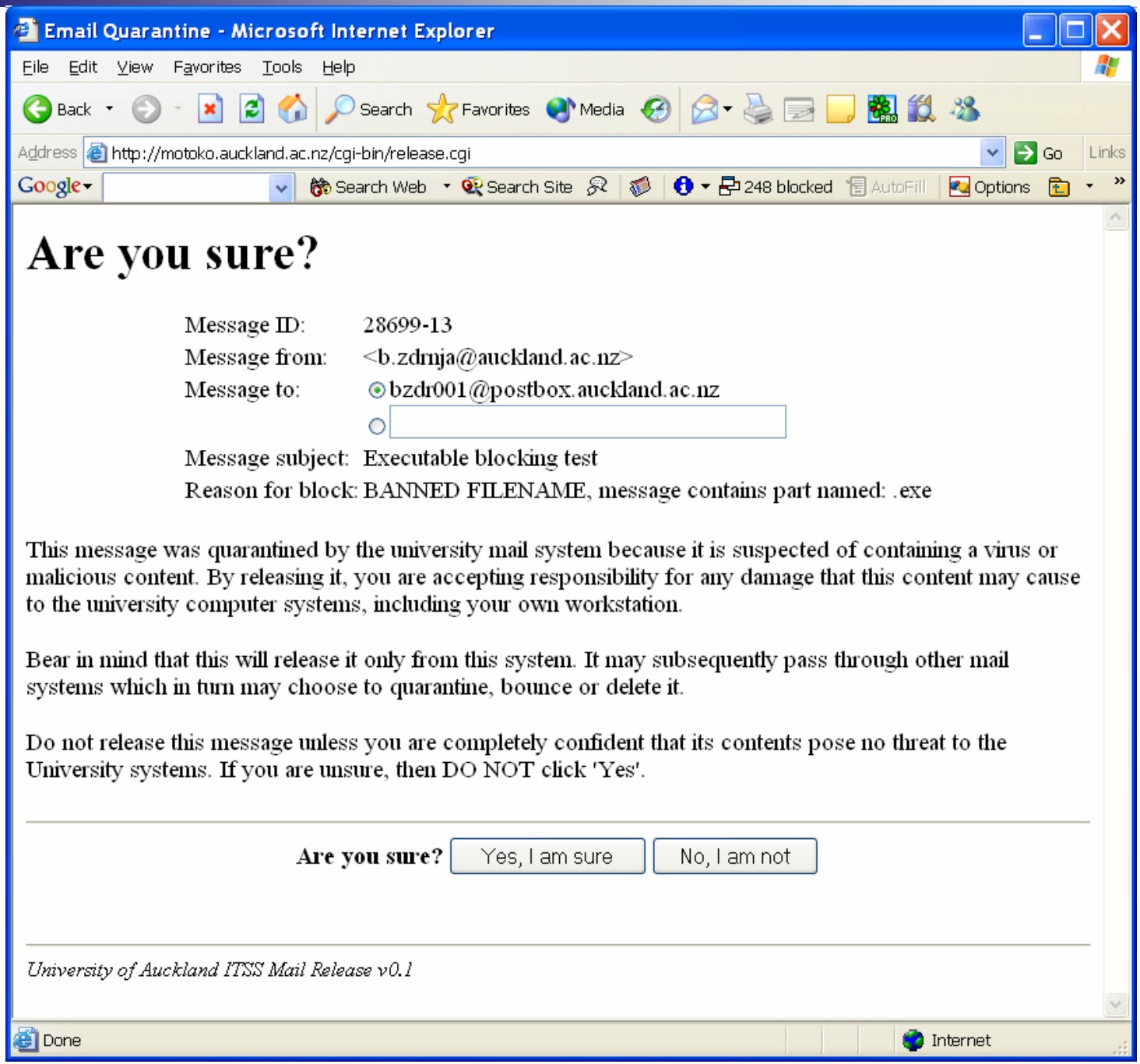
.

Steganography



AV detection and policy

- User requests Service Desk to release of quarantined file
- Service Desk uses Web interface to release file
- Messages kept in the quarantine for one month (quarantine size is ~700 MB)


Email Quarantine - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://motoko.auckland.ac.nz/cgi-bin/release.cgi
Go Links
Google Search Web Search Site 248 blocked AutoFill Options
Are you sure?
Message ID: 28699-13
Message from: <b.zdrnja@auckland.ac.nz>
Message to: bzdr001@postbox.auckland.ac.nz
Message subject: Executable blocking test
Reason for block: BANNED FILENAME, message contains part named: .exe
This message was quarantined by the university mail system because it is suspected of containing a virus or malicious content. By releasing it, you are accepting responsibility for any damage that this content may cause to the university computer systems, including your own workstation.
Bear in mind that this will release it only from this system. It may subsequently pass through other mail systems which in turn may choose to quarantine, bounce or delete it.
Do not release this message unless you are completely confident that its contents pose no threat to the University systems. If you are unsure, then DO NOT click 'Yes'.
Are you sure? Yes, I am sure No, I am not
University of Auckland ITSS Mail Release v0.1
Done
Internet

Spam detection

- Currently hot topic
- Many users fail to understand the difficulty
- It’s not simple to detect spam reliably
- Same approach as always in security: use multiple layers

Spam detection (why is it hard?)

- HTML e-mail helps spammers a lot
  - **Various rendering tricks evade filters**
- US CAN-SPAM Act
  - **After the act, amount of spam increased!**
  - **Also known as I-CAN-SPAM Act**
- The goal is to make spam sending expensive for spammers

Spam detection (tests)

- External tests (we use almost all available!)
  - Standard RBLs
- Vipul's Razor
- DCC (Distributed Checksum Clearinghouses)
- SURBL (SpamCopURI)

Spam detection (learning)

- Probability analysis classification
- Bayes (SpamAssassin)
  - **Autolearning mode for high score spam**
  - **Same for ham as custom rule gives -150 score to UoA messages**
- Dspam
  - **Initial manual learning**
  - **Still experimental in our system**

Spam detection (learning)

- **Only one statistical base for whole system**
- **SA and Dspam run under one user**
- **We theoretically lose a little on detection, but system learns faster now**
- ***Subject: V1AGRA: buy 0n1in3 n0w***

Spam detection (scoring)

- Each test adds to the final score
- Current threshold is 5.5
- Locally generated mail gets -150 to avoid false positives
- Experimental feature of dropping e-mail with score more than 10
  - Still in test phase, e-mail just logged

Spam detection (results)

- Excellent results
- Positive feedback from users
- System detects daily around 60.000 spam messages
- Estimate around 500 false negatives
- This gives final spam detection ratio of 99.17%!

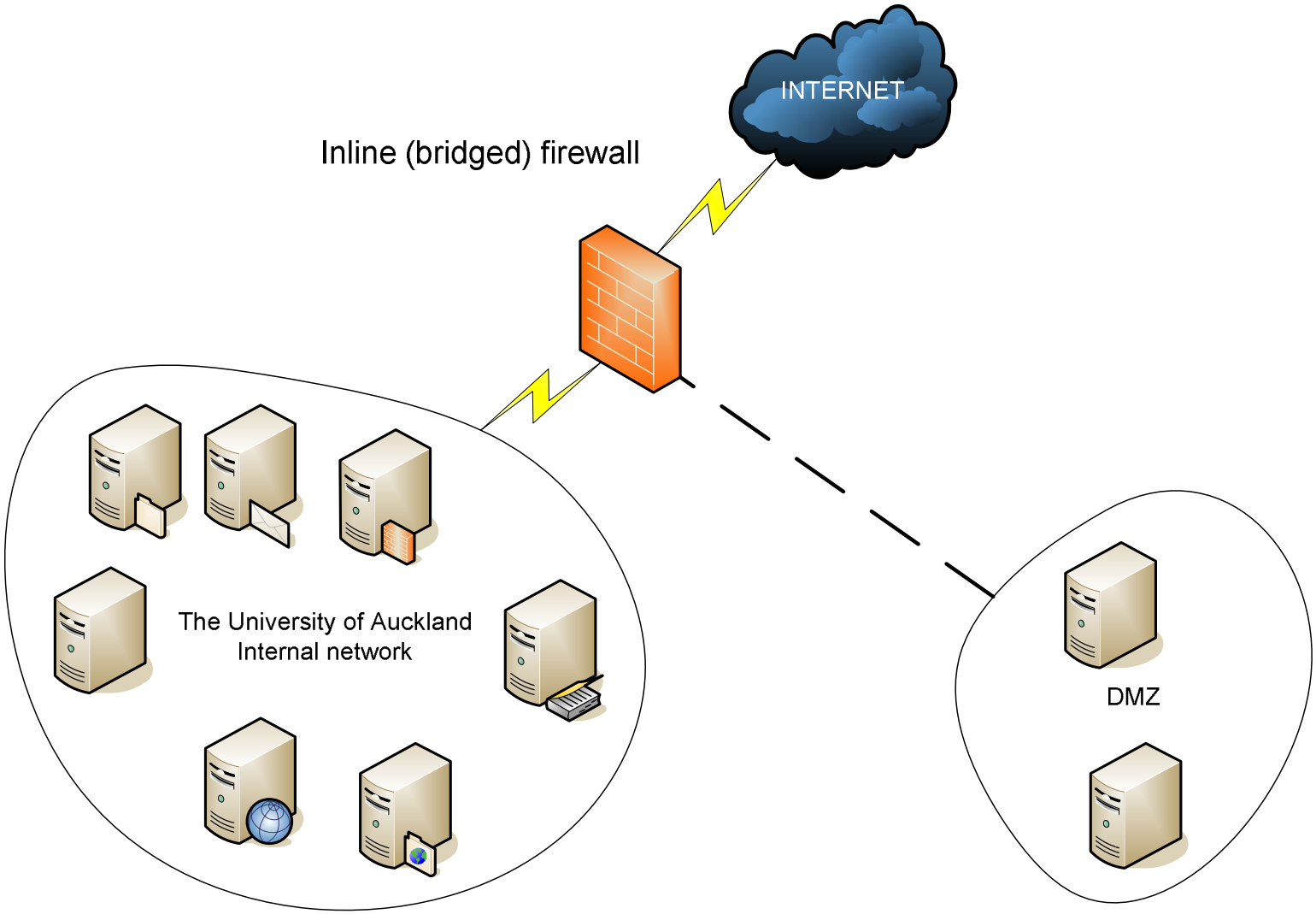
Spam detection (future)

- Encapsulation of detected spam into attachment with description of tests
- Installation of local servers for some collaboration tools (SURBL) to speed up queries
- SPF (Sender Policy Framework)
- Grey listing?
  - Maybe, but clashes with users request for “instant” e-mail
  - Spammers will find way around
- How to make spam sending expensive?

Protecting hosts

- **Firewall incoming ports unless they are needed**
  - **only 600 of 7500 systems have incoming ports open**
  - **block MS related ports: 135—139 & 445**
  - **faculty IT Staff control FW configuration**
    - They are close to the users and understand their needs
    - They are the ones who usually have to clean up after compromise
- Get host patched promptly
  - **easier said than done**
  - **not covered in this discussion**
- Desktop AV
  - **doesn't stop attacks**
  - **will stop worms installing themselves**

Architecture



Detecting infections

- UOA has long monitored traffic entering and leaving the network for suspicious activity
- We are now deploying similar monitors within the campus network
  - used both for security monitoring and network trouble shooting
  - Linux based
- Argus & Watcher – http://www.qosient.com
- Snort – http://www.snort.org
- SmbLure – http://www.utdallas.edu/~pauls/smblure/
- tcpdump/ethereal – basic network capture and analysis

Argus and Watcher

- Argus is a network traffic audit tool
  - **records data about flows passing the monitoring point**
- Data may be written to disk or piped to another process for further processing
- Watcher reads data generated by Argus and looks for patterns that indicate scanning
  - **Written by Russell Fulton, distributed with Argus in perl contrib package**
  - **Emails alerts to Faculty IT staff when it detects suspicious traffic**
- Argus data kept on disk for two months
  - **useful for figuring out what happened after the fact**

Snort

- Network based IDS
- Deployed on internal network and DMZ
- Uses signatures to detect known attacks
- Automatic signature updates – we use our own perl script but oinkmaster is also good
  - **http://oinkmaster.sourceforge.net/ (author Andreas Östling – su.se)**
- view/report events with Placid
  - **http://speakeasy.wpi.edu/placid/ (author Phillip Deneault – wpi.edu)**
- Acid is an more powerful but slower alternative
- All NIDS prone to false positives

SMBlure

- Traps worms that spread via windows based shares
- Runs on any Unix system that supports Samba
- Works by creating an open share with a facsimile of a windows C Drive
  - named so that it will be at the top of most browse lists
- Comes with scripts that analyse samba logs and anything attackers leave on the share
- Reports findings by e-mail

How to deal with infected machines

- Get them off the network ASAP!
  - **We notify Faculty IT staff automatically**
  - **A comprehensive database of switch port/IP/MAC address info will allow us to quickly locate machines by IP**
  - **Big plus for static IPs!**
  - **Last resort: we kill off switch ports if we can't locate the machines**
  - **Wireless, VPN and Dial-in users pose special problems**
  - **As are laptops on the wired network**

Wish list

- Network login (already implemented for wireless dial-in and VPN access)
  - **Check machines at login for current AV, patches, etc.**
- Ability to bar machine based on MAC address, particularly for mobile machines
- Better detection and notification tools
  - **http://netsquid.tamu.edu/details.html ??**
- Automatic vulnerability checks on connection, particularly for mobile and dial-in/VPN devices

Summary

- Be good netizens – fight spam and malware effectively in your back yard and save the 'Net!
- To be effective you must be both proactive and diligent
- You must also invest resources, particularly people time
- Many effective tools are open source

Questions?

- Contact:
- Russell Fulton
  - r.fulton@auckland.ac.nz
- Bojan Zdrnja
  - b.zdrnja@auckland.ac.nz