mancalanetworks

making networks manageable

Networkshop 2011

2011-04-12

Introduction

mancalanetworks
making networks manageable

What we do now

- Why it doesn't work
- It really doesn't work
- Use-cases

What we can do about it

- Integration
- Use all of the information at our disposal
- Enforce network security, don't detect it.

How many systems do we need?

mancalanetworks
making networks manageable

Networks are complicated

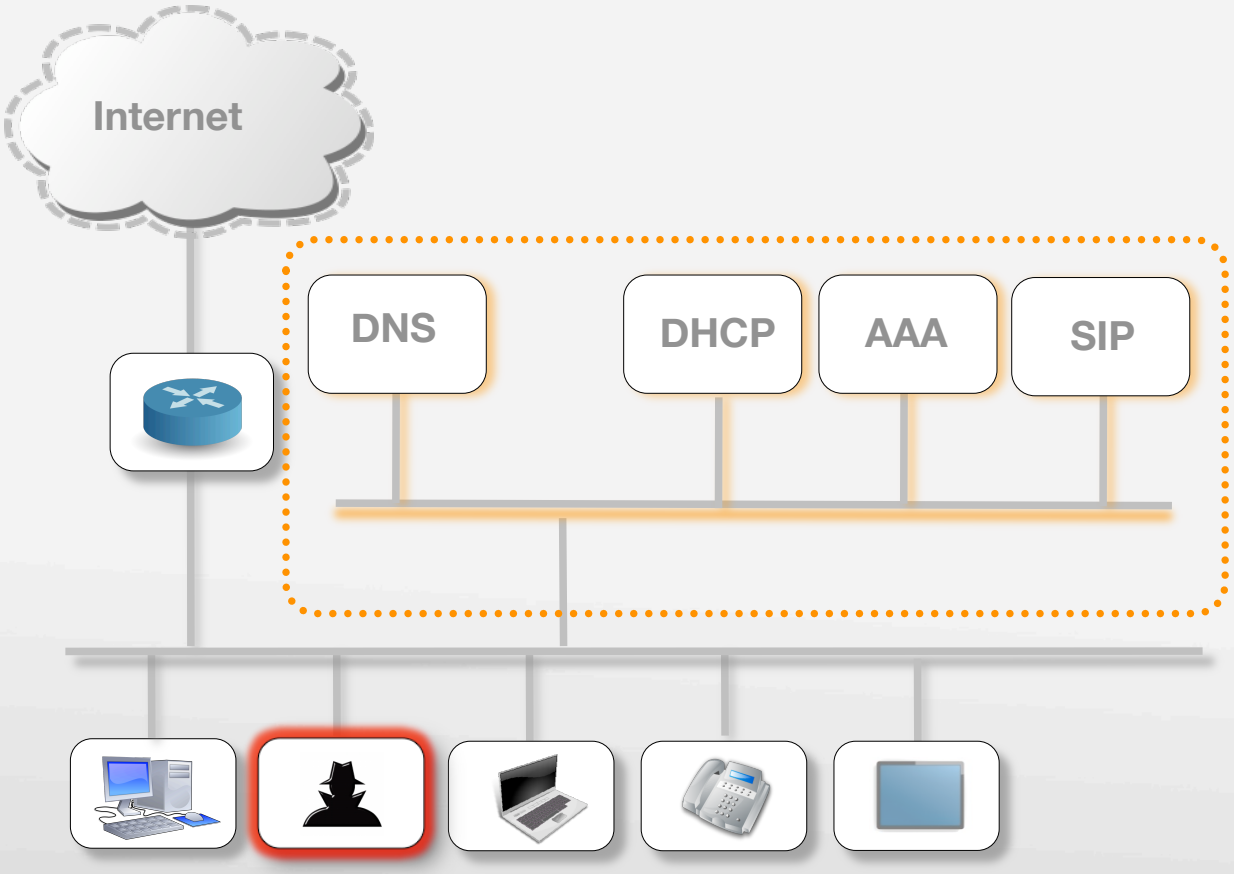
1 RADIUS for authentication

1 DHCP for addresses

1 DNS for name resolution

1 TFTP for VoIP phone booting

1 SIP for voice



They all manage the same users and devices

It gets worse

mancalanetworks
making networks manageable

Branch offices

Mobile workers

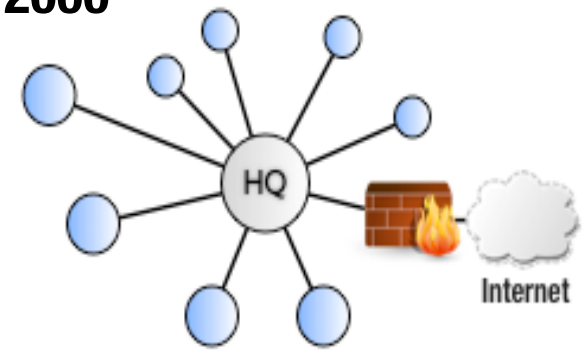
Devices

Threats

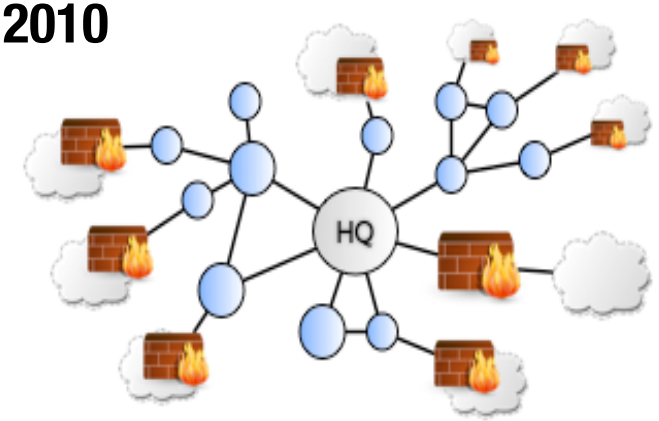
Regulation

Networks are more complicated than ever

2000



2010



Attacks are more sophisticated

mancalanetworks
making networks manageable

Branch offices

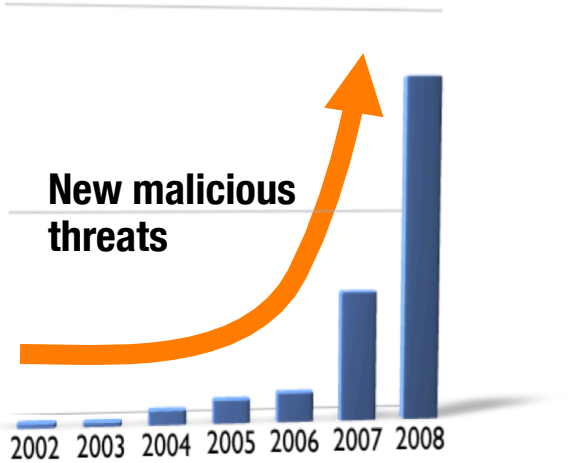
Mobile workers

Devices

Threats

Regulation

Emerging threats



Number 1 driver for investing in security solutions is
to stop threats from propagating

(Infonetics Research, 2009)

What can we do?

mancalanetworks
making networks manageable

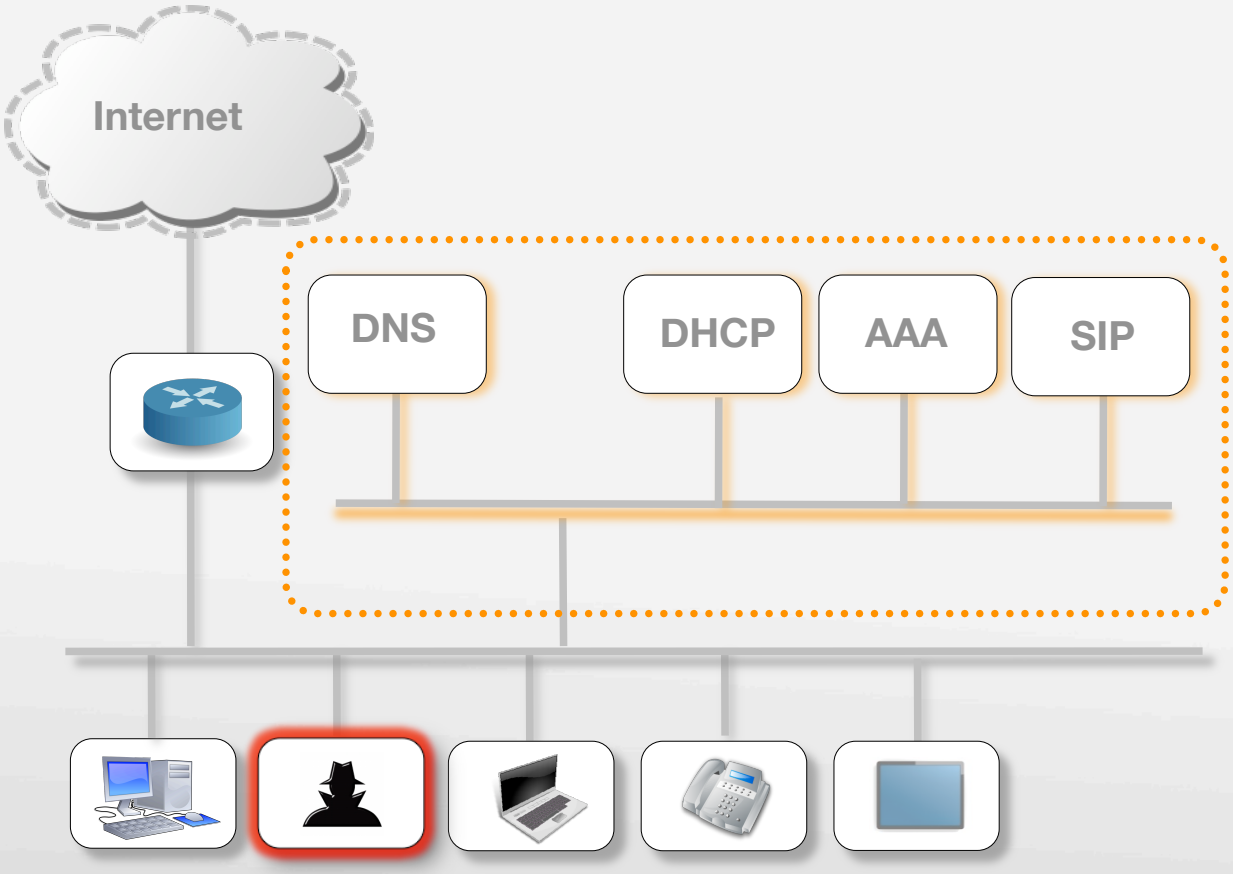
Administration is complicated

1 Different vendors

1 Different protocols

1 Different databases

1 Different administration interfaces



A unified response is a consistent response

Integrated network management

mancalanetworks
making networks manageable

What we can do

- Extending the security boundary of the LAN to the network edge
- Unifying authentication, location, identity, permissions
- Enabling critical security concepts such as identity, location, and device security posture to be introduced to network management

But…

What about mobile users connecting to authenticated networks?

What about non-authenticating devices like printers, product scanners…?

What about the trend toward the “consumerization” of IT devices?

What if I use PXE Boot or Windows deployment services to provision my devices?

The catch : it all becomes harder to manage and secure

… unless you integrate your systems

Use case: Device Profiling

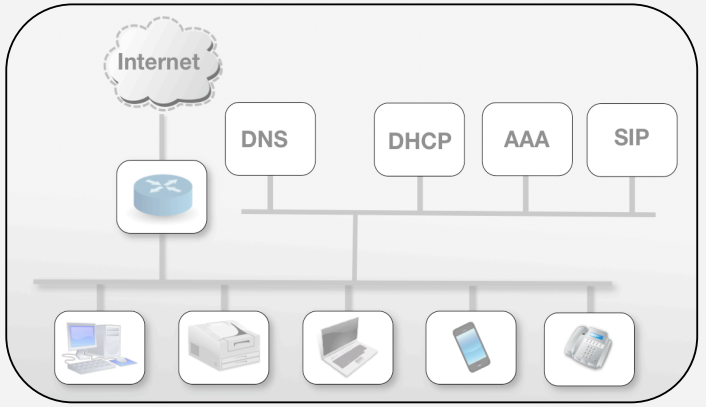
mancalanetworks
making networks manageable

Configured state:

- 802.1X plus MAC auth for 802.1X incapable devices

Observed view:

- Use DHCP + NMAP, etc. to create profile



Enforcement Mode:

- Leverage RADIUS, DHCP, VMPS, etc. for enforcment
- Detect MAC spoofing by comparing current data to historical data

Use Case: Is it a printer?

mancalanetworks
making networks manageable

How do you know?

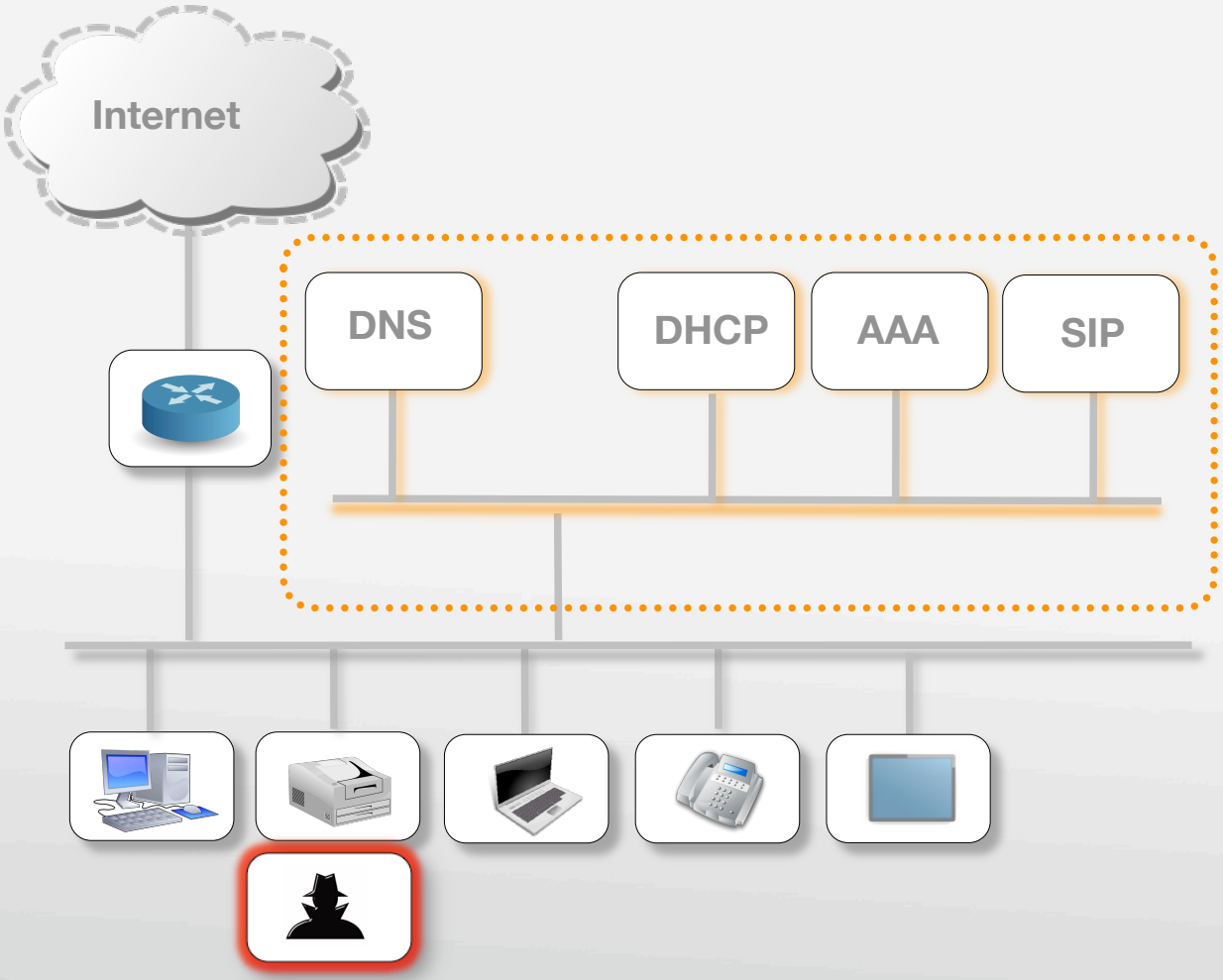
1. It looks like a printer
1. It does printer type things
1. It doesn't do non-printer type things

RADIUS MAC Auth

DHCP fingerprinting

NMAP

Other techniques



A comprehensive device profile fits in a DB

Use Case: VoIP Phones

mancalanetworks
making networks manageable

Why is the phone outside?

1 Phones have a location

1 Enforce it in RADIUS

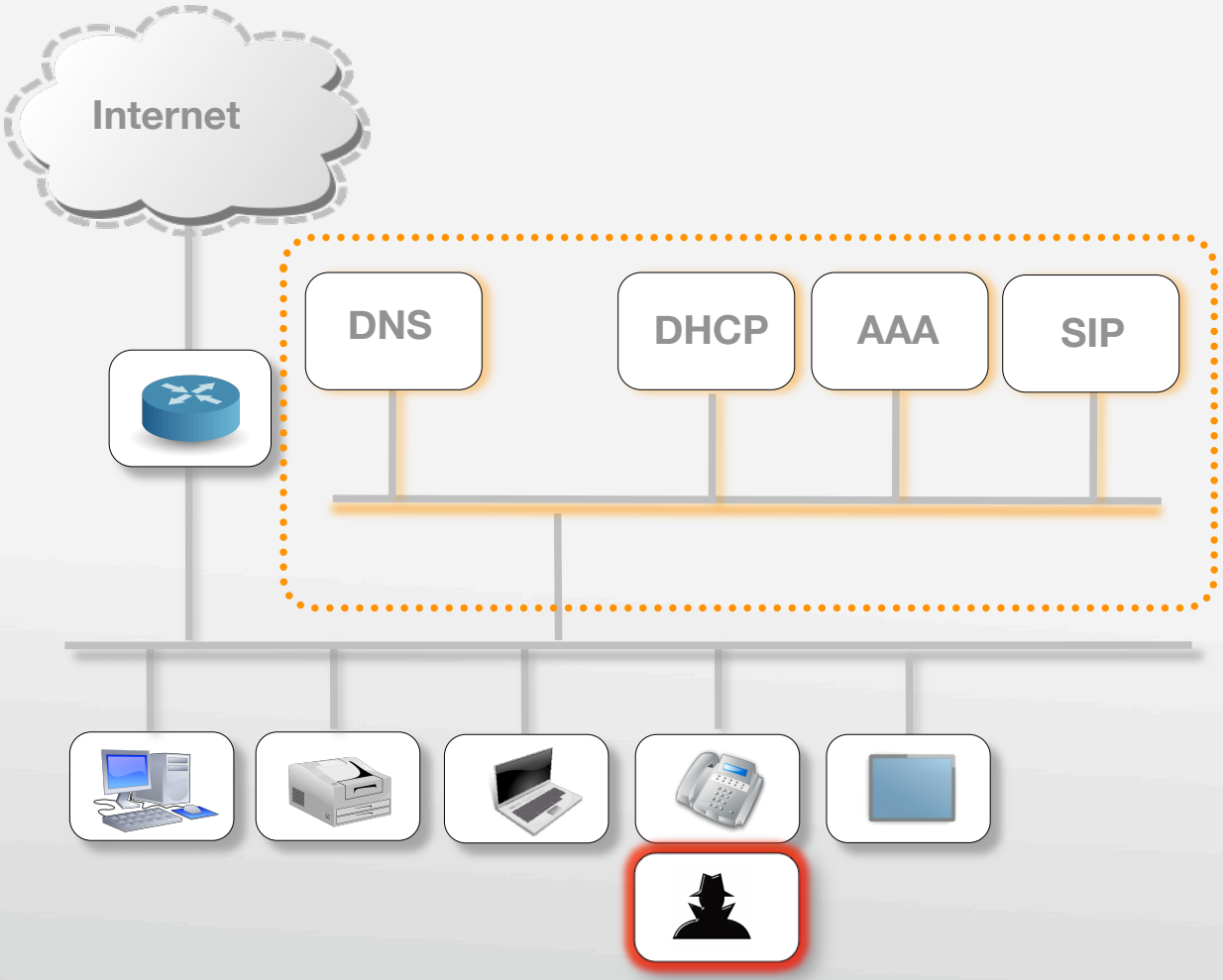
1 SIP Server gains security !

MAC + Switch IP/Port

Device type

User account

All done in RADIUS



A device profile allows enforcement

Similar projects

mancalanetworks
making networks manageable

Packet Fence

- Already does some DHCP
- Some FreeRADIUS Integration
- Missing VMPS

OSSIM

- Inventory isn't good enough
- Enforcement is required, too

What you need to do

mancalanetworks
making networks manageable

Integrate everything

- Use a database to store all information about the network
- Look up that information for every networking protocol
- Do cross-correlations
- Look for inconsistencies

If you don't do it, the attackers will

- DNS “private IP attacks”
- Stealing VoIP phones
- Inconsistency means a higher attack profile

What we're doing about it

mancalanetworks
making networks manageable

Releasing code

- Much better DHCP integration into FreeRADIUS
- Postgresql only for now
- Scripts to convert ISCP DHCP configurations to FreeRADIUS / SQL

Developing new code

- ARP plugins (why not?)
- Starting to work more closely with PacketFence
- More CoA and SNMP work
- “kick user offline” becomes protocol independent

And more

mancalanetworks
making networks manageable

Doing it all

- TFTP, ARP, SNMP, DHCP, DNS, RADIUS, HTTP(S, VMPS, TACACS+
  - No Diameter!
- Captive portal, VLAN
- Integrated network debugging
- Global policy enforcment
- SQL, LDAP intregration
- Active Directory
- FreeRADIUS + Web UI + SQL integration

mancalanetworks

making networks manageable

Questions ?