Broadband Network Insecurity & Implications

A white paper by the consultants of Matta Security Limited

http://www.trustmatta.com

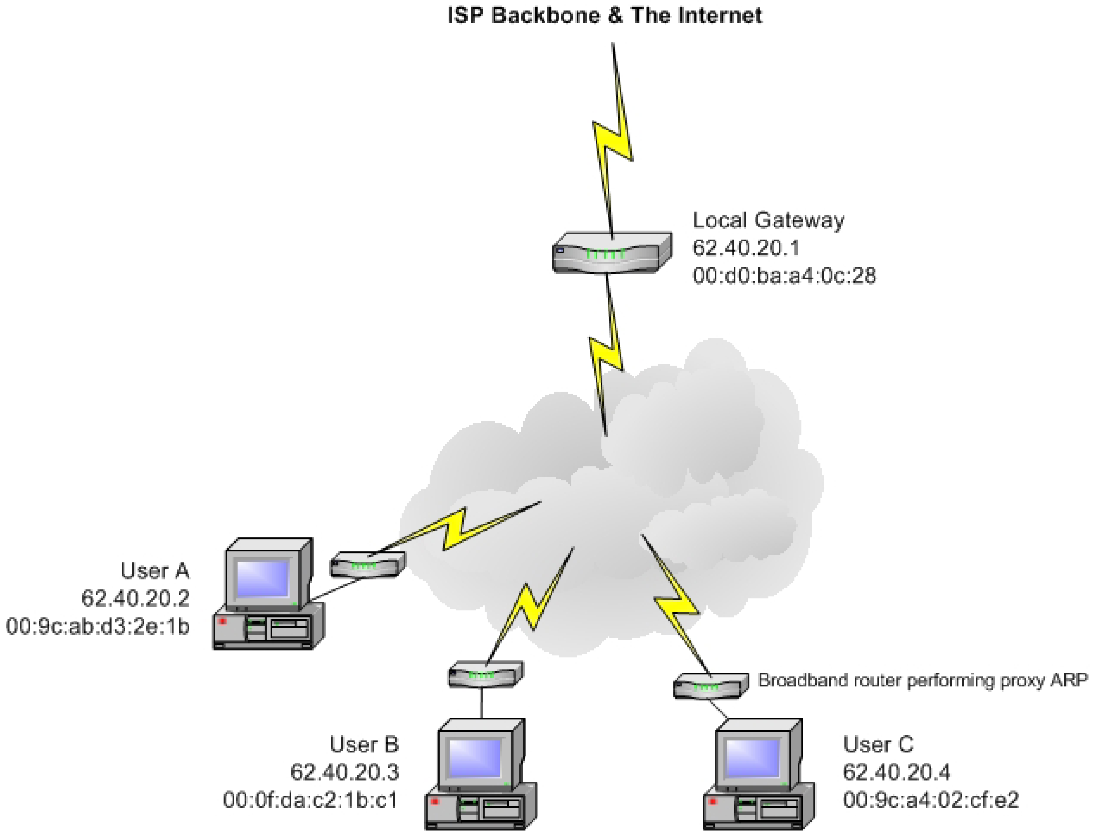
+44 (0) 8700 77 11 00

Introduction

As broadband Internet access is widely introduced throughout the United Kingdom, users realise a permanent Internet connection through which they can telecommute, use online banking, and purchase products and services using secure SSL channels. This white paper discusses the technical security issues around broadband, which also apply to many internal corporate networks.

Matta has realised through investigating network security of broadband Internet providers, that all traffic (including encrypted SSL / HTTPS) flowing across a local network segment can be compromised and sniffed, allowing for localised attackers to siphon sensitive information from other broadband users and systems. Even VPN tunnels can be attacked & compromised using this type of attack, depending on the key exchange and negotiation processes used. For the purposes of this paper, we will concentrate on the impact to the consumer using the Internet to purchase goods and connect into corporate networks.

Broadband Logical Network Topology



A simple network diagrams depicting three PC's connected to the Telewest broadband network.

ARP

ARP (Address Resolution Protocol) is used in all Ethernet / IP networks to resolve IP addresses to physical device addresses. ARP is not routable, and so vulnerabilities within ARP can only be exploited by malicious users with access to the local network segment (through either owning a broadband connection, or compromising a remote host that is connected through broadband).

In our above example, if User A was to issue an *arp –a* command, then the contents of the machine's ARP cache will be shown:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>arp -a

Interface: 62.40.20.2 on Interface 0x1000006
  Internet Address      Physical Address      Type
  62.40.20.1            00-d0-ba-a4-0c-28     dynamic

C:\>
```

62.40.20.1 is the default gateway for User A, and so any Internet bound traffic will be sent to this address and routed through Telewest's network and out to the Internet. The actual network that we undertook security testing on had a 255.255.255.0 or /24 subnet mask, and so was home to a total of 253 broadband users, each set to use the same default gateway of 62.40.20.1.

Sweeping the Local Segment

First a sweep of the local network segment was undertaken in order to identify active hosts. Nmap was used to first perform a simple ping sweep, which effectively populated the ARP cache of our workstation, and gave insight into poorly protected neighbouring systems:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>nmap -sP 62.40.20.0/24

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host s03-ule02-ma.blueyonder.co.uk (62.40.20.1) appears to be up.
Host pc-62-40-20-3-ma.blueyonder.co.uk (62.40.20.3) appears to be up.
Host pc-62-40-20-6-ma.blueyonder.co.uk (62.40.20.6) appears to be up.
Host pc-62-40-20-7-ma.blueyonder.co.uk (62.40.20.7) appears to be up.
Host pc-62-40-20-9-ma.blueyonder.co.uk (62.40.20.9) appears to be up.

  (3 pages of results omitted for aesthetic purposes)

Host pc-62-40-20-245-ma.blueyonder.co.uk (62.40.20.245) appears to be up.
Host pc-62-40-20-247-ma.blueyonder.co.uk (62.40.20.247) appears to be up.
Host pc-62-40-20-249-ma.blueyonder.co.uk (62.40.20.249) appears to be up.

Nmap run completed -- 256 IP addresses (91 hosts up) scanned in 94 seconds

C:\>
```

Nmap is freely available for download from http://www.insecure.org/nmap/nmap_download.html

We then take a look at our ARP cache:

```
C:\>arp -a

Interface: 62.40.20.2 on Interface 0x1000006
  Internet Address      Physical Address      Type
  62.40.20.1            00-d0-ba-a4-0c-28     dynamic
  62.40.20.3            00-0f-da-2c-1b-c1     dynamic
  62.40.20.4            00-9c-a4-02-cf-e2     dynamic
  62.40.20.5            00-40-f2-4c-21-1e     dynamic
  62.40.20.6            00-10-a6-05-f1-93     dynamic
  62.40.20.7            00-30-ae-0f-d8-72     dynamic
  62.40.20.9            00-08-02-8b-af-ef     dynamic
  62.40.20.15           00-07-e2-c4-a2-51     dynamic
  62.40.20.16           00-03-9a-7b-3a-fa     dynamic
  62.40.20.19           00-02-e4-1f-13-ca     dynamic
```

From reviewing the contents of the cache we get accurate details of our neighbouring systems, even if they don't respond to ICMP ECHO request packets. Immediately we see that 62.40.20.4 and 62.40.20.5 have physical addresses but did not appear in our initial *ping sweep* results; this indicates that they are probably using personal firewall software to filter dangerous packets.

Statistics collected from the local segment for a given day in December 2002:

- 91 neighbouring PC's identified by our initial *ping sweep*
- 189 physical addresses in total identified (local network at 74% capacity)

Sniffing the Network

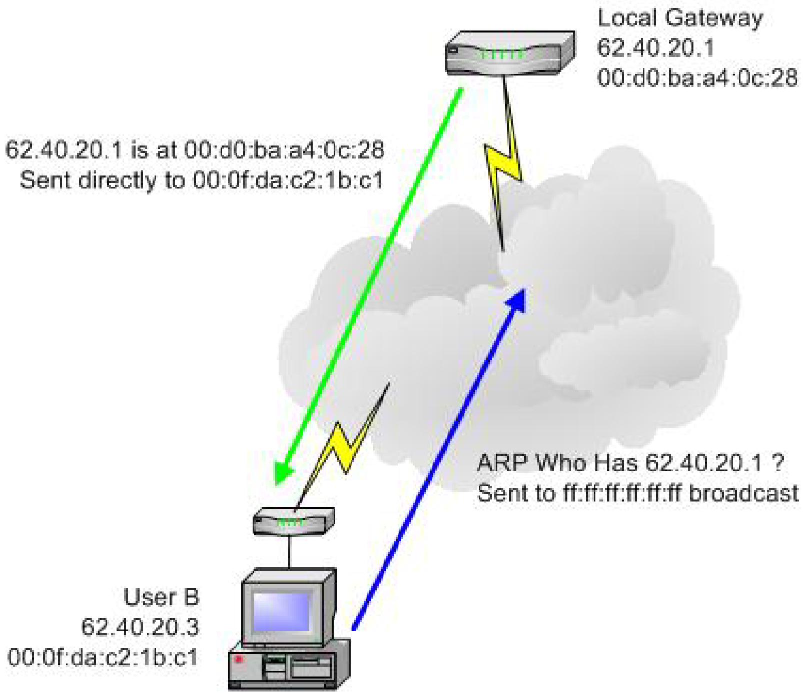
Initial sniffing using Ethereal will only show the following traffic:

- Traffic from your PC to the Internet
  - Web requests, login information for FTP, Telnet, POP3, et al
  - Outbound e-mail messages
- Traffic from the Internet to your PC
  - Inbound web content, images and text
  - Inbound e-mail via. POP3
- IP broadcast packets to 62.40.20.255
  - Windows NetBIOS broadcasts for naming queries
- Ethernet broadcast frames to ff:ff:ff:ff:ff:ff
  - ARP requests and replies

Due to switching within the broadband network, casual sniffing by placing the PC's network card into *promiscuous mode* does not allow us to compromise traffic between neighbouring systems and the Internet. The same results would be seen if you were to attempt to sniff network traffic within any switched network (such as internal corporate environments). Many technical network managers and systems administrators believe that switched networks are invulnerable to sniffing and session hijacking attacks, which is not the case.

Using ARP to Compromise Traffic Flow

ARP is the protocol used in all Ethernet / IP networks that allows local machines to resolve IP addresses to physical device addresses. Below is an example of an ARP process when a machine wishes to initiate a TCP/IP connection with another local host:


Local Gateway
62.40.20.1
00:d0:ba:a4:0c:28
62.40.20.1 is at 00:d0:ba:a4:0c:28
Sent directly to 00:0f:da:c2:1b:c1
ARP Who Has 62.40.20.1 ?
Sent to ff:ff:ff:ff:ff:ff broadcast
User B
62.40.20.3
00:0f:da:c2:1b:c1

All mainstream operating systems (Windows, Linux, MacOS, et al) use ARP caches that are dynamic. Dynamic ARP cache entries are updated and refreshed as requests for physical address details from the local network are fulfilled. ARP is stateless and does not perform any authentication, and so fake ARP replies can be sent to hosts in order to poison dynamic ARP cache entries.

ARP cache poisoning can be used by an attacker in two ways:

- Denial of Service (DoS), by convincing the target workstation that the MAC address for its default gateway is a non-existent one. When the user attempts to browse the Internet or initiate any outbound connection, it simply won't work.

- Redirection of traffic, by convincing the target workstation that the MAC address for its default gateway is infact that of the attacker's workstation, and then forwarding the traffic accordingly. A redirection attack can be undertaken completely seamlessly; due to resilience within TCP/IP the victim's active network connections will not be reset.

A Windows tool that can be easily used to perform ARP cache poisoning and redirection is ARPsniffer.exe, by a Chinese programming and hacking group called netXeyes. To prevent backdooring of the program, we have mirrored it along with the WinPcap drivers required, at http://www.trustmatta.com/services/docs/ARPsniffer.zip

Using ARPSniffer

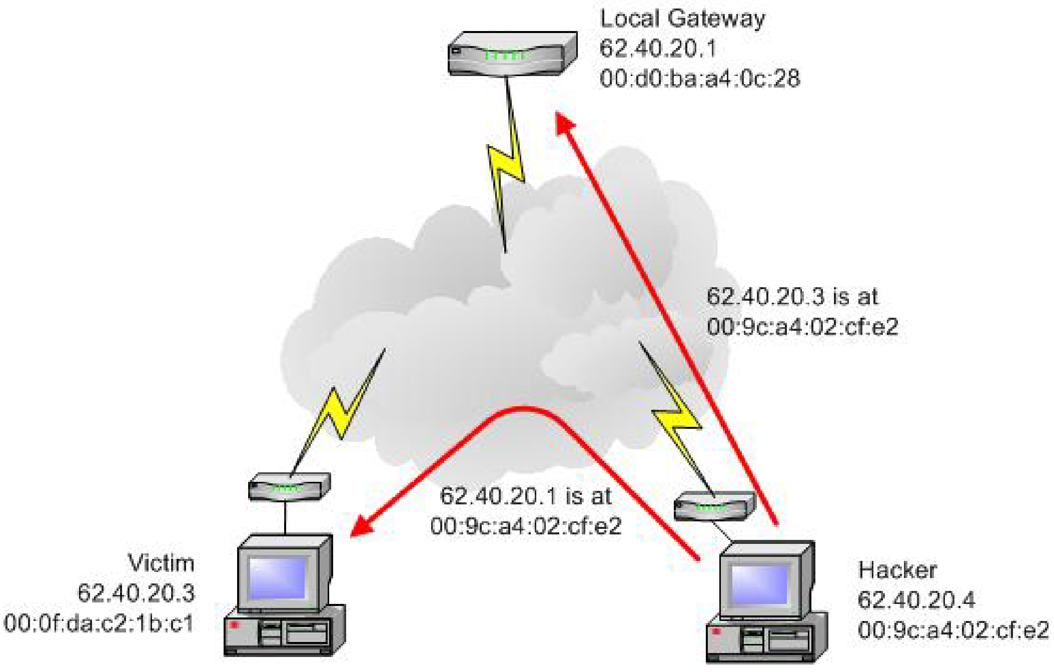
The ARPSniffer program has the following usage:

```
C:\>arpsniffer

ARPSniffer 0.5 (Router Inside), by netXeyes, Special Thanks BB
www.netXeyes.com 2002, security@vip.sina.com

Network Adapter 1: Intel(R) PRO/100 VE Network Connection
Network Adapter 2: NETGEAR FA330/FA331 PCI Adapter

Usage: ArpSniffer <IP1> <IP2> <Sniffer TCP Port> <LogFile> <NetAdp> [/RESET]

C:\>
```

We give the program the following arguments:

- The two IP addresses that we wish to intercept traffic between
  (for example a default gateway such as 62.40.20.1 and an end user system such as 62.40.20.3)
- A chosen TCP port to intercept the traffic of
  (for example port 110 for POP3 e-mail interception)
- A log filename
- The number of the network adapter we wish to carry out the attack through

The ARPSniffer utility then proceeds to run in the background, performing ARP cache poisoning of both the end user workstation at 62.40.20.3 and the default gateway at 62.40.20.1:



When the victim at 62.40.20.1 sends and data outbound to the Internet, it will flow through the hacker's machine first, and then be forwarded to the gateway. Inbound traffic from the gateway to the victim will also be sent through the hacker's machine.

Sniffing ARP Redirected Traffic

Now that traffic flows through our PC, we can sniff and analyse it. The ARPSniffer utility only has the capability to sniff traffic to a single TCP port, and so we must use a powerful sniffing package such as Ethereal, a WinPcap-based sniffer for Windows and Unix-based platforms alike, available from http://www.ethereal.com.

Through using Ethereal in this way, we will see all traffic flowing between the victim host and the default gateway. Plaintext data in particular will be immediately compromised, including:

- All HTTP traffic
- Instant messenger, IRC and chatroom data
- Telnet, FTP, and other plaintext service passwords
- Outbound and inbound e-mail (SMTP and POP3)

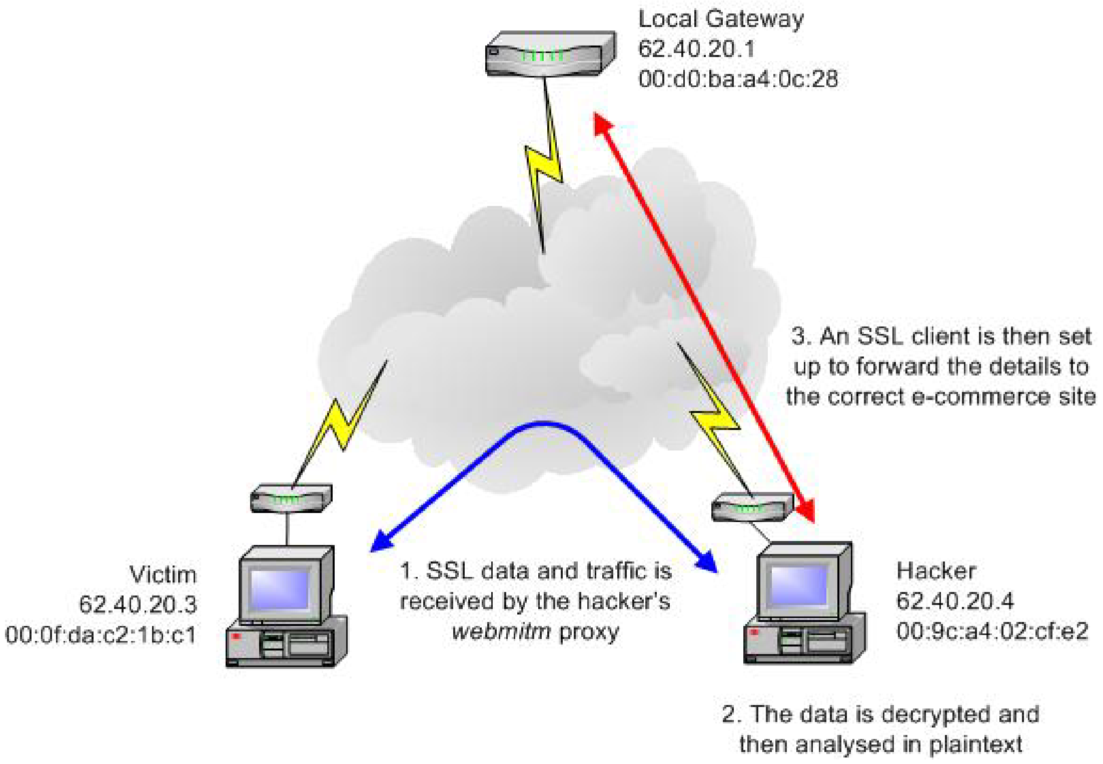
Encrypted traffic will not be compromised by performing just ARP cache poisoning and sniffing using Ethereal, but seamless encryption types such as SSL (used in virtually all online e-commerce and banking environments) can be compromised by launching a man in the middle attack.

Man in the Middle Attacks

A man in the middle attack to compromise SSL protected information flowing across a broadband cable network involves the following being undertaken:

- ARP cache poisoning and redirection of traffic
- Using an SSL man in the middle program such as the *webmitm* utility found in Dug Song's Dsniff package (available from http://naughty.monkey.org/~dugsong/dsniff/)

The *webmitm* utility is used as a transparent HTTPS (TCP port 443) proxy, so that when our victim then attempts to connect outbound to an e-commerce site or online bank, he is really communicating with the hacker's SSL proxy, which then passes his credentials and data to the real e-commerce server or online bank:


Local Gateway
62.40.20.1
00:d0:ba:a4:0c:28
3. An SSL client is then set up to forward the details to the correct e-commerce site
Victim
62.40.20.3
00:0f:da:c2:1b:c1
1. SSL data and traffic is received by the hacker's *webmitm* proxy
Hacker
62.40.20.4
00:9c:a4:02:cf:e2
2. The data is decrypted and then analysed in plaintext