KPMG: On Covert Channels in Networks and Eavesdropping Communication Note

The aim of this chapter is to provide an insight as to how organisations, multinationals, governements etc. incorporate security within their network and/or lack of security. Points shall also be illuastrated with some technical explanations of relevent security topics.

1.1.**Covert Channels: Secret Communication that passes your network security**

In todays world, data loss is a hot topic. Guarding ones data is already hard and is getting harder to achieve. USB sticks, lost login credentials, wireless accesses, unknown network entry points and others are all sources of information leak. Such channels may or may not be known. The goal of this section is to learn about covert channels. Gain insight into how they can be constructed with current techniques and what tools and options are at a hackers disposal. Moreover failures caused by an over reliance on technical measures shall be explored.

1.1.1. What is a Covert Channel?

The United States Department of Defence (1985) defines covert channels as being:

i. a communication channel that allows a process to transfer information in a manner that violates the system's security policy.

under the proviso of using existing, visible,known and normal transport. Thus the traffic of a covert channel over regular communication and data transport channels, is visible, within known protocols and looks like normal traffic. It can be a single system that operates a mutli-level security policy. Here the focus shall be on network based cover channels.

1.1.2. How do they Work?

such as IP and ICMP. This gives them the appearance of being visible, known and normal. Three ways in which one can construct a covert channel are using:

IP

In an IP packet header the ID field (16 bits) should be random, the options field (24 bits), is not used in most common situations and the padding (8 bits) should all be zero. These fields can be used to hide information.

ICMP

Here the data field, which is arbitrary in length can be used to hold and thus hide information.

DNS

In a DNS request the ID field (16 bits) is used to keep track of queries made. The QD, AN, NS and AR fields are used to store, the number of: questions, resource records in answer, name servers received in answer, answers respectively. These fields can be used to store information. While DNS can be used it requires an algorithm to coordinate all the necessary changes needed. For instance with QNAME, which is the actual query, its max length is 255 bytes. A max of 63 octets per label. DNS implementations can choose to ignore the contents of QNAME, same with ANSWER field.

Encoding Information

When encoding information it is a trade-off between value and transition, with regards to the dimension, it is a trade-off between spatial versus temporal. Spatially, the value can be a letter in bits, transition will represent the change from one value to another. Temporally, the value represents the arrival of a packet, and transition represents the transition of arrival of a packet. These can be used to encode information properly on the covert channel.

Theory

The path of a covert channel can be Direct, going straight from host to host in a {single hop}, Indirect, going through several hops via several proxies or {bounce hosts}or Spread in which the destination of the channel consists of several end-systems. Covert channels can exhibit two types of behaviour: Passive — when they piggy back on the traffic of other processes; or Active — when they generate their own traffic. Other aspects to consider is the efficiency of the channel, it is always a trade-off between space and time. Synchronisation might all be needed as well as separate control and data channels.

1.1.3. Demo

A demonstration of a covert channel that utilises HTTP(S) for shell access to a system and the use of tunnelling via DNS can be found located at https://alumni.os3.nl/~marcs/covertchannels/.

1.1.4. Implementations in the Wild

Covert channels are not new and there are a lot of existing implementations, many with easy installers. Some examples include:

IPv4 Covert_tcp sob

IPv6 V00d00n3t

DNS Ozyman nstx DNScat

HTTP firepass corkscrew cct

MSN MSNShell

A lot of malicious entities use covert channels for nefarious means, however information is sparse and rare to comeby. Examples of use include the DDoS tool Stacheldraht (1998) that used ICMP for control and the PrettyPark Worm (1999) that used IRC. It is predicted that in the future one will see other covert channels emerging such as those based upon the Skpye API, IPv6, HTTP(S) and even torrent based channels.

1.1.5. Where do we go from here?

None of the actions performed through the established of covert channels run against the specification as laid out in the RFC. Properly implemented protocols should and do allow the use of covert channels. Their detection does not necessarily mean their prevention. Worse still is the use of temporary channels, who's use is intermittent.

To detect covert channels and thus identify and confirm their existence, protocol anomaly detection will work. Thus excessive behaviour can be spotted e.g. continuous pinging and enormous DNS resolving. Each of the tools used will have various characteristics. For example, DNS tools use txt records. ICMP tools use specific payload field. The replay of a DNS Query doesn't provide the same answer and finally HTTP(s) should have short requests and Long answers.

1.2. Listen and Repeat — Eavesdropping DECT

The Digital Enhanced Cordless Telecommunications (DECT) protocol, is a propriety protocol (Implying that manufacturers have to sign an NDA) that facilitates wireless data and voice communication. Created in 1992, it is used in a variety of situations and settings such as Cordless phones, Wireless ISDN access, baby-monitors, remote door openers, traffic lights etc. Germany alone has approximately 31.5 million DECT enabled devices. Dect operates over the 1880-1900 MHz band (EU) consisting of 24 slots for each of the ten channels. TDMA, TDD and FDMA. However due to a lack of synchronisation sniffing becomes possible.

Table 3. Abbreviations

FP	Fixed Part (base station)
PP	Portable Part (handheld)
RFPI	Radio Fixed Part Identity (Hardware address of the device)
RSSI	Received Signal Strength Indication (Signal strength of the base station)
Repeater	Range extender
DSC	DECT Standard Cipher (Encryption cipher)
DSAA	DECT Standard Authentication Algorithm
UAK	User Authentication Key (master key between FP and PP)

Characteristics

Base station

RFPI broadcast active, base or repeater mode, PRNG is determining the strength of the UAK, broad ranges are possible and optionally is the use of encryption and PIN services.

Handheld

No RFPI broadcast, it initiates the connections, when used initiates encryption (optional), and dialing is predominantly unencrypted.

1.2.1. Security of DECT Devices

The DECT Standard specifies the use of DSAA as a mandatory option and that DSC is optional. Authentication (pairing) is achieved through use of DSAA, the A11 algorithm is key to the security. UAK has a key strength of 64-bit though a 128 bit (RAND and Key) is used. The PIN can be used as part of the key and the real key space can be considered to be around 36.5 bit. Encryption is achieved via DSC, but depends on the security of the UAK. Due to a licence issue no open source implementation is available. UAK defines the minimum dimension of security. There are problems with hard coded UAKS, PRNG is mostly weak and easily computable.

Security of Base Stations

When securing a base station it is paramount that a strong PIN be used to authenticate the handheld. But how does one choose a strong PIN? How complex should it be? and How often should authentication occur, after switching on the device? Base stations should enforce DSC encryption and offers access protection of the admin interface, though this is mostly web based.

Security of Handheld

A password/PIN is used to protect the handhelds configuration, similarly a PIN is used for the authentication of the base against the handheld though this is rarely seen. Questions to ask are: Is the DSC encryption enforced (aka Downgrade attack)? and Is the dial number transmitted unencrypted?

1.2.2. Attack Scenarios

To attack DECT one simple needs to acquire a 50 euro DECT Card i.e. Dosch & Amand Type 3 or 3, a notebook running linux and some drivers from http://dedected.org.

Sniffing the Communication

For this attack some engineers reversed engineered the Dosch & Amand stack. As they did not know the DECT protocol, they were able to write a linux driver that enables the card to log all DECT communications. It hops through all the channels and hooks onto a communication channel if a device is detected. The card can synchronise with a device by detecting the agree time slots i.e. hopping interval. This techniques can also lead to the impersonation of a base station with a rogue base unit. There are problems when intercepting the communication between repeaters.

Repeaters are used to increase coverage of larger areas. Often the communication between them is not encrypted. Thus communication can be intercepted between the repeaters.

Breaking UAK: DSAA Analysis

From the ETSI non-disclosure agreement for the DSC:

6. Not to register, or attempt to register, any IPR (patents or the like rights) relating to the DSC and containing all or part of the INFORMATION.

However U.S. Patent 5,608,802, registered by Alcatel, originally registered in Spain in 1993 states:

A data ciphering device that has special application in implementing Digital European Cordless Telephone (DECT) standard data ciphering algorithm

Oops! There is a paper detailing several paper attacks on the DECT authentication mechanisms, it has been accepted to CT-RSA-2009. The paper details and provides an analysis of DSAA. C and Java implementations will also be available onhttp://dedected.org. There is a high performance VHDL for FPGA cards but it is still closed source.

DECT Jamming

Using a Siemens gigaset:

1. Switch it off.

2. Press 1 4 7 simultaneously when powering it on.

3. Press 76200.

4. Select SAR in the menu and choose the biggest option i.e. 1 slot/1slot low/2 slot.

5. Select the channel according to the following options: LOW=0, CENTER=5, HIGH=9.

Wardriving reloaded

Through the use of WarDriving techniques it was found that DECT devices are detectable far outside the range of the required environment. Thus the attacker doesn't need to be inside the house to perform an attack.

1.2.3. Countermeasures

There are several countermeasures that one can utilise:

1. Use strong PIN-Codes (if possible)
2. Disable {Repeater Mode}
3. Use device protection (screen locker)
4. Protect the base station (physical)
5. Enforce encryption (choose the right manufacturer and model)
6. Do not use DECT where Security is needed (it´s only 64(36.5)-Bit)

1.3. Network (In)security: What is seen in practice!

1.3.1. What Companies struggle with?

All companies struggle with: Knowledge and Thinking.

Knowledge

It still hard to find someone who knows it's networks basics and understands security of systems and networks, and preferably also understand what security is about.

Thinking

Thinking in as many boxes as possible. Companies have got many, many departments. IT is spread across groups for network, support, Windows/UNIX server, desktop, database, SAP, etc.

Large size companies also struggle with aspects such as De-perimeterisation, this is when the defined perimeters of an organisation are less strict due to more mobile devices such as blackberries, laptops etc. Ever expanding networks, tools such as Chilli can be used to detect any unwanted extrusion and allow tests to ensure that extrusion cannot happen. More over is device configuration and monitoring in terms of ensuring compliance and managing devices on a large scale. Hackers (and creative)

people are hard to counter, they are most of the time, more resourceful than security engineers.

1.3.2. Real World Examples

Some examples of what has been seen at clients include problems including: Network Segregation Default passwords, everything connected to the Internet, angry personnel, bad policy enforcement, single account usage, running sessions, thinking in boxes for security and more depressing, no knowledge concerning the Internet and networks. Mind this list is not exhaustive…

Default Passwords

The service provider installed some process control equipment that has been given temporary default passwords and recommends that the passwords be changed. Some do not change these passwords, which are easily found on the Internet.

Network Segregation

Imagine a retail company installed a wireless network in shops and offices. WPA2-enterprise is used to control access to the wireless network. There is older equipment that cannot handle WPA2-enterprise so a legacy WLAN, WEP was activated. This resulted in no network segregation and the WEP enabled WLAN was hacked and access to all financial applications and checkout systems were granted. Even more so the inside systems were not patched…

Angry Employees

Imaging sliced network cables… Imagine a small company, when leaving an IT Administrator changes the password on all devices in the company…

Policy Translation

Security Policies should be easily enforced, maintained and implemented. There has to be the right control for the right task. For example:

- Cryptographic keys need to be at least 512-bits — Problem: not clear. Is this for symmetric keys (a bit long for 3DES)? or Is this for a-symmetric (a bit short for RSA)?
- Only authorized workstations may be connected to the network

- Problem: How are you going to enforce this?
- the firewall should generate an alarm for unauthorized logins
- Problem: How do you know a login is unauthorized…?

One Account

Imagine there is a single account for management processes. For all management processes. This account needs to be kept secure.

Session Left Open

Windows domain is pretty good when it is secured however, when it is not i.e. Bastion Server, then RDP and admin/password credentials can be found. Thus root sessions are instigated, hence banking systems and password hashes from all other core systems.

Security thinking in boxes

Most people tend to think about security in terms of boxes, that is login via the Internet, web portal links to a certain service and only that service. Which implies limited system access. Which is not actually the case.

NooB

These are people with no knowledge of the Internet and networks in general. They might think that a switch is too slow, do not know how to log on and tends to think: It was expensive so it should work!.

1.3.3. Our deduced Findings

Security crosses layers and boundaries that normally people tend to isolate and contain. Boxes and layers are wrong! The most simple and effective countermeasure is through Network Segregation, but it is rarely utilised.

Source: http://jfdm.host.cs.st-andrews.ac.uk/notes/netsec/#_security_attacks