Exploring Protocols and Services on Internet Connected Embedded Devices

The Context of CCTV's as Embedded Devices on an IP Network

Security Rules for the Masses

- Security products are Secure
- Existing Technologies are Secure
- Passwords = Security
- IP Address Filtering = Security
- A Firewall = Security
- Professional Security Services = Technical Security

Private Investigations

- CCTV, VoIP, Video Conferencing oIP, and TV oIP all involve the use of Embedded Devices to a great extent
- Each one of these types of Devices will account for a greater percentage usage of total bandwidth than all previous Devices put together
- Each of these uses, or will use existing Protocols and Services regardless of their maturity for security
- What a massive Potential for Private Investigations!
- What a Potential for Storage Services
- What a Headache for Security, Privacy and Data Protection

Today's Aim:

- Create an interest in the future of Embedded Devices by understanding the Context of present and past Practices
- Offer Pointers on exploring Technical insecurities by looking at CCTV's in a non-technical approach – You can all learn the technical stuff easily, the non-technical knowledge I have gained is not so easy

My background

- Spoken to Police and Local Authority Managers on Benchmarking the Security of Network CCTV Systems
- In January speaking at IIPSEC 2006
- Auditing CCTV Systems
- Database of CCTV Cameras based on a Spider
- Vulnerabilities of Critical National Infrastructure's use of Network CCTV Systems
- Research Database of Embedded Devices

What I will be Covering

- The uses of Embedded Devices
- Communicating Embedded Devices
- Example of CCTV as a Communicating Embedded Device
- Exploring Embedded Devices can be Fun
- Identifying some of the Vulnerable Protocols and Services in IP based CCTV Systems
- The basis for discussion on the importance of Securing Communicating Embedded Devices in your Organisation the same as any other Devices
- Why the Context is More important than the Technology, (You can't get Context from Manuals or Web Site)

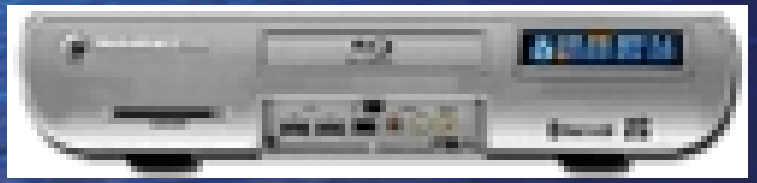
What I won't be covering

- How to Hack an Embedded Device
- How to find CCTV Cameras or WebCams
- Exploiting Vulnerabilities
- Technical workings of anything I cover
- Risk Assessment of either CCTV Systems or any individual Embedded Device
- How to Select Communicating Devices
- Standards (Communication, Encryption, Compression, Graphics & Images)

Content

- Embedded Devices Types, Uses
- Why Embedded Devices are Interesting
- IP based CCTV Systems - Context
- Components of CCTV Systems - Context
- It can be Fun and Easy to Explore CCTV Systems
- Protocols and Services in CCTV's - Context
- Are the Vulnerabilities in Internet Connected Embedded Devices any Different from any other Network Devices? - Context
- The Future - Context

Examples of devices?



Uses are all around us:

- Consumer
- Manufacturing, Automobiles
- Military
- Medical
- Office Automation, Communication
- Security, Access Control & Surveillance
- Network Monitoring

Why look at Embedded Devices

- Embedded devices taking Centre stage
- The coming Internet Connected revolution
- Independence of Embedded Devices
- Increasing Reliance on Embedded Devices
- They will / do Control what you can / cannot do
- They Will soon be used to form mini networks managed by other Devices designed to specifically to manage that type of network
- Is Embedded Device Security maturing for this future role

What Makes ED's Interesting

- They usually fulfil a very specific need
- They are usually assumed to be as secure as necessary
- If they are physically Secured they are often unattended
- Many are remotely controllable out of the Box
- Many have lots of cool un-documented or un-considered features
- The super-computers of yesteryear are the ED's of Today What about Super-Computer of Today?
- No Different than other Network Devices, except maybe less secure!

Advantages of using ED's

- Often have a very Specific Purpose
- And have very Specific Functionality
- Can Reliably be left to work independently without and intervention (once conf. app.)
- Can be left on once powered up

Are there any Downsides?

- Let's take a look at what can be done, by using CCTV's as an example
- Lack of knowledge in Configuring them without additional Technical Assistance
- If it has to be controlled remotely it is open to network Insecurity
- Connecting a Device to the Network means using existing Internet Services & Protocols

A flying tour of how we got here

- Need for Simple Devices
- Chips
- Operating Systems
- Consumer Devices
- Modems, Cisco, 3Com, etc.
- Mobile Phones
- PDA's
- Military, Manufacturing,

Trends leading to the Future

- Chip Technology
- RAM Chip Technology
- Communication Applications
- Killer Applications
- Greater Uses
- Price
- Consumer Demand

How much more of what we already have?

- ?m Mobile Phones
- ?m MP3 Players
- ?m Network Devices
- ?m Wireless Network Access Hardware
- ?m Robotic Hardware

What will be connected to the Internet in the future?

The Question should be “What wont be connected to the Internet?”

How these were and are connected

- Open Wireless
- Open Wired
- Closed Network
- Depend on use and proximity

Let's look at CCTV Systems

- I'm not covering searching for Live CCTV Cameras, or WebCams in any great detail.
- This topic is covered by other sites:
- www.i-kacked.com/content/view/81/42/
- http://wonder.i.am/
- www.griffid.com/?page=livecams
- Also, there was a session earlier today

The Earlier CCTV Session

- Was very Interesting, even though it was given in German but with English Slides
- For those English speakers that missed it, get the slides when they come out
- One of the Personal Privacy Techniques they mentioned was using a Laser Pointer
- Another was Laser Hat

WebCam/CCTV – What's difference

- Image quality
- Direct / Indirect Connection to Network
- Availability of Hardware and Software to expand Functionality
- Remote Control Functionality
- Therefore requirement of other functionality

What makes 16m Cameras for 60m people so important?

Their Security! (Security of the Cameras not the people

CCTV's in the UK

- There are 16m Cameras for 60m people
- Yet still increasing in the UK
- Replacement Cycle now on; closed for IP based
- UK is often cited as a world-wide example of successful use and implementation
- Success of Identifying and following movements of the London Bombers
- UK has a lot of expertise!??!
- Perspective – UK population 60m

Networked CCTV Research

- Database compiled using Spiders
- Benchmarking the Security of CCTV Systems
- Vulnerabilities of Network CCTV Systems in the Critical National Infrastructure
- Vulnerabilities Matrix for devices with Embedded Systems

First of all, forget the technology

- – It all starts with physical security stupid – this applies to all devices not just those that are portable

IP based CCTV Systems

- Closed System
- Simplest – Home network
- Part of internal Network
- Stand-alone Internet Camera

Closed System

- When they first came about Closed Circuit Television Systems were actually Closed
- They required Camera and Viewing Station to be Close, due to the Cabling, or to use Optical Cables
- Could not take advantage of Digital Technology easily
- So midway / complete Digital IP Systems

OK So Let's Explore IP Systems

- Network Setup
- Internet Setup
- What Protocols & Services can we observe
- Complication of Standards

What Does a basic CCTV System need to do?

- Convert image into a format which can be transmitted to a monitoring device
- Record for future viewing
- Controlled Remotely
- Use and work with existing Communications Technology

A CCTV Management System must:

- Enable management of a large number of cameras Remotely
- Control Recording, Access to Recording
- Viewing of Data

Networked CCTV Components

- Camera (OS, Application, Chips)
- Image Manipulation Software (conversion, compression)
- Management Software (Unit and System)
- Viewing Software
- Recording Hardware
- Recording Software
- Many ways to Implement

What about Security Components

- These are secondary to the System Functionality!!?
- Let's take an example look at a Successful Vendor's offering

Let's look at Axis Systems

- At www.axis.com
- Possibly Market leaders
- Either typical of functionality or leading in functionality
- Provide plenty of information on the site
- Let's take an approach a Hacker may take looking at this information with the aim of identifying what is worth exploring for exploit purposes

Web site provide:

- Sales Product Data
- Product Technical Data
- Manuals
- How to Documents
- Examples
- Most Importantly, Firmware Upgrades

What are the recommended Setups

- Simple Home Setup (very few – not their main market yet)
- Remote Network Setup (simple / Complex)
- Local Network Setup

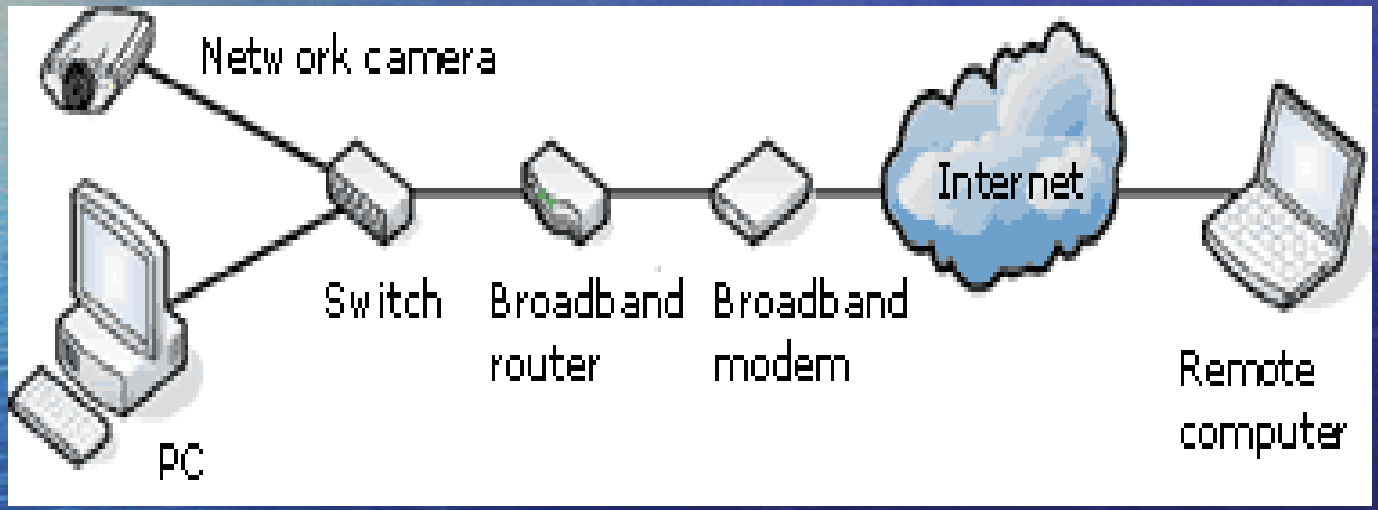
But what is the likely reality?

- Most systems were installed 1992-1998
- For those installed 1998-2000 …
- For those installed 2000-2005 …
- For those being installed now …
- Whatever is not on the web site, can be searched in the Google archive

Older Technology / Management

- Analogue to Digital
- Multiplexers
- Most Schemes run by Police and Local Authorities
- Installed by CCTV Specialists no Networking Experience
- Many Mixed Systems in Use today
- Not built for Security but for functionality (just like so many current technologies)

Remote Network System Setup



Cameras Technologies

- Control – Pan, Tilt & Zoom
- Remote Camera Control
- Remote Viewing
- Remote Audio
- Remote Upgrading for Software
- Day / Night Use
- Compression
- Intruder Sensors
- Image Conversion
- Email Notifications

DVR's, Viewing Systems, etc.

- Local / Remote Recording (Tape / CD / DVD / Hard-disk)
- Multiple Camera Recording (timed, random, etc.)
- Programmed / Manual / Automated
- Event Based
- Image based

Camera Setup

- Check Manual and Firefox

Making it Work Axis Web Site 1

- Show Manual and Web Site

Software Downloads Axis Web Site 2

- Show Manual and Web Site

Managing Systems Web Site 3

- Show Manual and Web Site

For Developers Web Site 4

- Show Manual and Web Site

What are the Services / Protocols 1

- Web Server Services
- FTP / TFTP
- SMTP
- SNMP
- IP TCP / UDP
- Dynamic DNS Service

What are the Services / Protocols 2

- HTTPS
- DNS
- Telnet
- Shell Scripting
- PHP Scripting
- Task Scheduler

Where are we up to - Technical

- Remote Cameras are not necessarily on the Local Network, so are not monitored as such
- No IDS / IPS, No Log files
- FTP recent many used TFTP
- No evidence of Login attempts
- Little or No encryption (HTTPS recent)
- Security: IP Address Filtering, multi-level Passwords
- Innovations in Scripting

Where are we up to – Non-Tech

- Specified by Non-Technical Staff
- Sold on Functionality
- Vendor's don't understand Security
- Vendor's aim to build Functionality for Interoperability
- Owned by Police and Local Authorities
- Installed by Non-Technical Staff
- Used by Non-Technical Staff
- Maintained by Non-IT Staff
- No IT Security Personnel Involved at any point

A Fist full of Vulnerabilities

- Where does one start?
- Always Stay legal – Quote from Chris Simpon
- Then, understand the background of the Scheme for which the cameras belong to, In England all Schemes must publish Scheme Data as part of Data Protection
- Then, well you know the rest
- Then test
- Oh yes Stay Legal

How CCTV's are different from other networked Devices

- They are often outside of the Network
- They may be internally listed on an External DNS Server
- The use of web servers leads to indexing by Google, you too are able to access them, all you need is to take a Google like approach.
- The use of SNMP and SMTP (in and outside the network)
- Scripting Tools
- Wide Range of Software available to achieve same end
- The implications of these clients and other clients on the network today and the future

Future CCTV Networks

- Single units will have their own databases of Rules for Intelligence
- Direct Connection to Larger Databases of Images of Wanted Individuals
- Creation of Event based Intelligence
- Connections with Other Biometric Technologies
- Connections with ID Schemes
- Replacing Passport Control? Maybe not yet
- Bigger Brother – Yes, for sure, in the interest of the Public of course

What future Devices must be able to deal with?

- Not just Spiders, worms, bots of today – talk of de-parameterization; but do so intelligently
- Intrusions
- Use as a Remote Hacking Device
- DDOS & DOS attacks
- Laser pointers and such interfering Technologies
- Breakdown of one component of the System
- Intelligent Group Co-ordinated Defence at Middleware Unit level

What about non-CCTV Devices, what Protocols and Services do they use?

- Vendors usually start with adapting existing Protocols, Services and Standards. Regardless of how Secure they are
- Sorry, Can't help on this one here, there is plenty of Information out there already – look at what we done with Axis

Future Approaches to Connecting Embedded Devices

- Device Connected Directly as a Single Secure Unit with IPS, Encryption, etc. etc.
- Devices Connected and Controlled as part of a larger Group / Unit by a New type of Intelligent Middleware Embedded Unit, creating a Mini-Network
- Similar Devices Connected as any other device but will be on their own sub-net using IP6

What can you do?

- Start with the Basics – Use Risk Approach
- Learn about the new Technologies, and their Protection before you are forced to learn about them
- Work with Vendors (if possible) to create better secure solutions
- Stay Legal! Have Fun – I'm sure Prison isn't Fun!

Other Interests and Research

- Secure Embedded Device OS (too many?)
- Security of Remote Controlled Wireless Devices
- Security of Databases on Embedded Systems
- Forensics of Image Tampering
- Buffer Overflows, Covert Channels

Questions?

- Contact me:
- sarbsembhi <at> blueyonder <dot> co <dot> uk

- Suspicion Breed Confidence – Brazil, Terry Gilliam