An End-to-End Analysis of Securing Network CCTV Systems

Sarb Sembhi

Hack in the Box 2007

My Background / Interests

- Developer / Project Manager
- Database / Web Based Development
- Learnt Security through the Development route
- Secure Coding
- Interest in Networked Hardware devices and their Software Security
- Research into Networked CCTV & Access Control Systems (hardware and software)
- E-criminal profiling

Why?

I like this photograph because it illustrates how the easiest way to break system security is often to Circumvent it rather than defeat it (as is the case with most software vulnerabilities related to insecure coding practices).
Robert Seacord: www.securecoding.cert.org

Session Objectives

- Background
- Role of CCTV (in Law Enforcement)
- Vulnerabilities in Implementation
- NOT going to cover the Why – I'll assume you know
- NOT going to cover details and specific exploits, attacks, technical vulnerabilities, etc.
- Will cover non-technical vulnerabilities that are inherent of such systems
- More slides than I'll cover, they're to show, this technology is no different than other technologies you work with

My Position / View of Security

- Secure Coding Framework
- Secure Data Framework
- Everything Else – (Architecture / Infrastructure)

What was and is CCTV

- Was – Closed Circuit TV
- Is:
  - Open, local broadcast TV
  - Open Networked TV
  - Closed Networked TV
- The last two are of interest to us in this session.

Open, Local Broadcast TV

- Transmits on specified bandwidths as agreed by local laws. (usually 1.2, 2.4, or 5)
- Short distances
- Technology used for baby monitors, etc.
- Used in Shop, Hotels, small businesses, Embassies!
- Technology used in low tech surveillance equipment
- Growing fast, sold as Wireless CCTV
- ? Is this really CCTV, and are we really having this discussion.
- Someone should get sued under Trade Descriptions!
- Used in Not-so-cool Cool toys

Open Networked TV

- Open to all
- Open to control by all
- Open with restrictions
- As Open as an Extranet

- This is the main topic of discussion

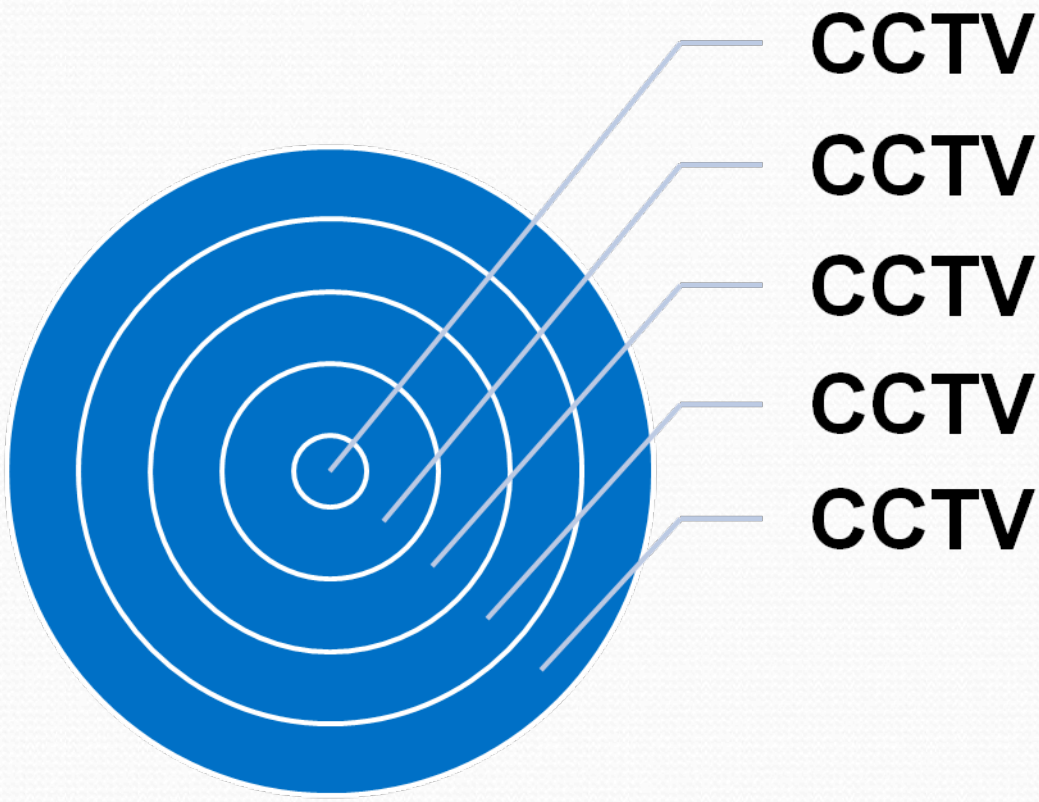
Closed Networked TV

- These are rare to find as it is like boxing a PC, in case someone attacks it!
- Why? Because they defeat some of the advantages offered by the Networking / Digital functionalities
- They do exist, but not in law enforcement
- Unfortunately, some exist due to ignorance of the installers, and sometimes politics
- They will usually be local, and using fibre optics (there's a clue)
- We won't discuss this in this session

Role of CCTV Systems (in Law Enforcement)

- Reducing Anti-Social Behaviour – you are being watched, we know who you are, we've seen you before, don't do it!
- Reducing Petty Crime – you won't get away with it, you're covered!
- Surveillance – you look suspicious, let's follow you covertly
- Identify and Search – ask for public assistance
- Evidence – OK we know you done it, here's the proof

Role of traditional Perimeter Security



CCTV Components

- Image Conversion (Charge Coupled Device, CMOS)
- Intruder Sensors
- Control – Pan, Tilt & Zoom
- Day / Night Use
- Remote Camera Control
- Remote Viewing
- Remote Audio
- Remote Upgrading for Software
- Compression
- Email Notifications (client / server)

Services / Protocols

- Web Server Services
- FTP / TFTP
- SNMP
- TCP / UDP
- DNS / Dynamic DNS Service
- HTTP / HTTPS
- Telnet
- Shell Scripting
- PHP Scripting
- Task Scheduler

DVR's Viewing Systems

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

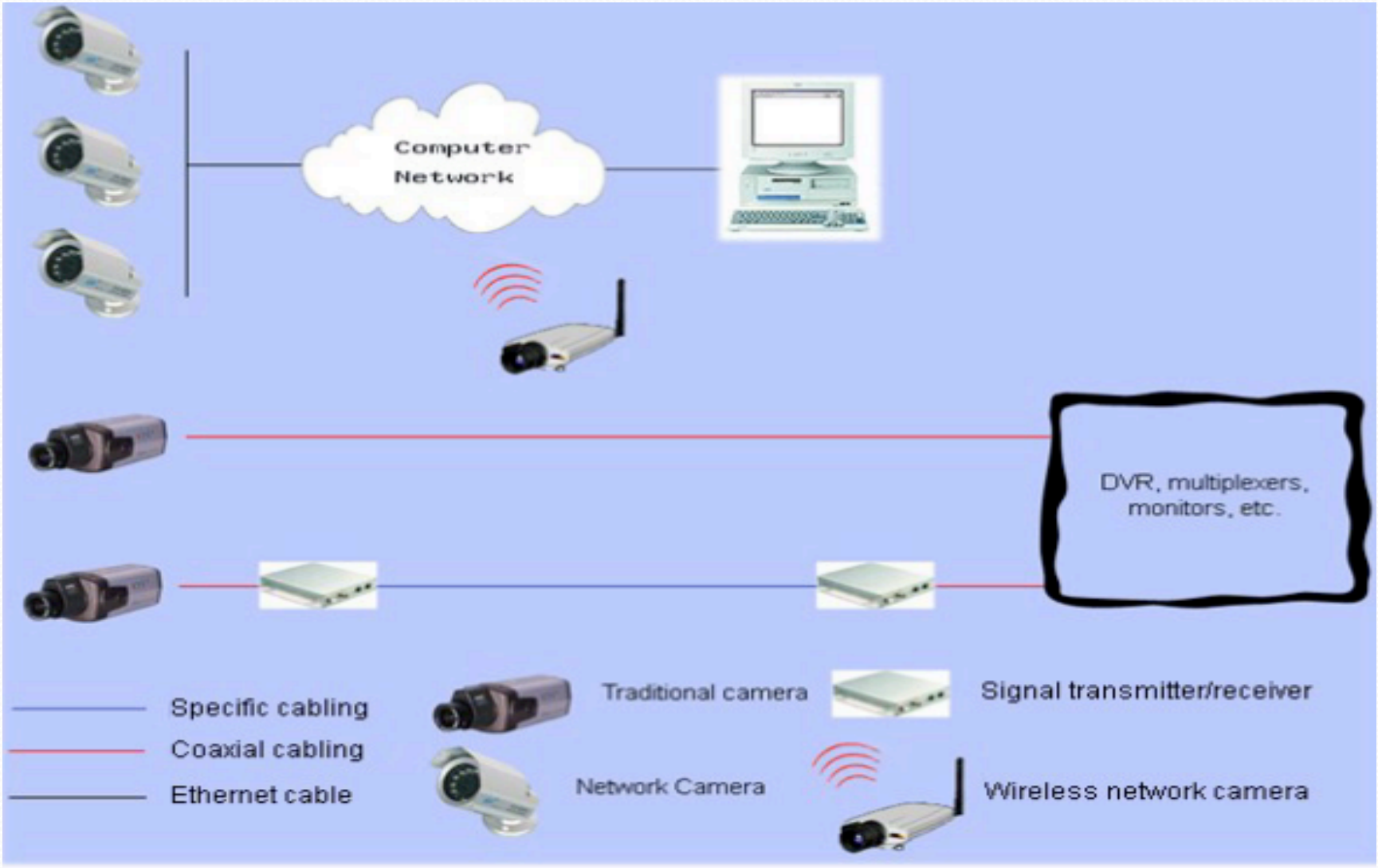


Figure 2 : Different topologies of a CCTV network

Network / System Components

- Network Card
- Wireless / Wired
- Switches
- Routers
- ? Firewalls (Only Cisco & big players)

Similarities with other Networked Embedded Devices

- No Graphical display
- Serves data
- Remote Controlled
- Security left to the Network level
- Embedded Operating System protocols and services

Technical problems areas

- Network
- Architecture
- Hardware
- Software
- Protocols
- Data Parsing

Implications of last few Slides

The Wrong focus

- Image quality
- Pan Tilt Zoom
- Recording
- Administration
- Even CCTV Forensics is not what I thought is would be

Sample Camera Unit Setups

- 1 : 1 (local)
- 1 : Many on a PC card over network (local)
- Many : Many on a PC (Networked locally)
- Many : Many (Networked Remotely)

Pulp Fiction Break

CCTV Implementation Issues 1

- Data Sharing (live and archived)
- Usefulness of Open / Closed
- Remote Control
- What is the Network?
- Current Network setup differences
- Whose is the Network?
- Installation (Security)
- Interoperable Technology
- Responsibility for different elements

CCTV Implementation Issues 2

- Control of System
- Recording (where it is based, type, etc.)
- Privacy (local laws)
- Alerts – who deals with them
- Lack of established Network Standards for secure installation
- Lack of Auditing / Pen Testing Approach
- Lack of Technical Network Maintenance and Support from Security perspective (from outset)

CCTV Implementation Issues 3

- Finance – who pays for the system
- Manufacturers – view of security!
- Installers – experience
- System Administrators Network knowledge

Basics

- Change the admin page
- Add a robot.txt
- Change & extend Password
- Ensure the use of a modal window for Password entry
- Separate from the rest of the Corporate Network
- Firewall
- Place in DMZ
- Change and Secure the things you can and place appropriate controls for the rest

The unfortunates of Securing end–to–end Networked CCTV

- Architecture
- Specification
- Data – secure according to risk
- Client Applications
- Network Monitoring
- People – Involve professionals
- Support and Maintenance

Take-aways from this session

- Since security is left to the Network level, deal with it!
- You can all do the Technology, it's not that New (it's anything but, in most cases)
- People are important, technology can't take over yet
- Policies, Procedures, Standards, Guidelines should also be set up just the same
- Plan & Organise like you would any other technology
- Test, Test, Test.
- Monitor, Monitor, Monitor
- Haven't we seen these things before, but why aren't people doing them for this technology!

Where are Manufacturers going with this technology?

- Wi-Max
- Mobile Phone Network
- Emergency Phone Network integration
- Behavioural Applications
- Greater integration to Databases
- Greater integration to other technologies (RFID, Biometrics, etc.)
- More SDKs'
- More PHP modules (more remote control)

Why the Excitement?

- Embedded Devices are the new PC's
- Embedded Operating Systems
- Embedded Networking Chips
- Embedded Encryption
- Embedded IPS
- Embedded databases
- Possibilities of Wi-Max

- All this equals lots of fun for the Security professionals

Where to from here – The Future (the Scary Bits)

- Integration of technologies (RFID and Biometrics) to CCTV's
- Open access to foreign governments
- Open access to criminals
- Growth – where did our privacy go
- Anything can be justified
- Back door into Networks
- "Just because I'm Paranoid, doesn't mean …."

Questions?

- PS, yes I would be interested if anyone wants to do some joint research or wants any direction.

Starting at the Start

- Understand your Hardware mix
- Understand your Data
- Understand your Technology Decisions
- Understand your Upgrade Path
- Understand your Requirements

Enforcing Security Policies

- Authentication
- Authorization
- Accountability
- Confidentiality
- Integrity
- Availability

Architectural Risk Analysis

- Learn & understand the target of analysis
- Identify and Discuss the software issues
- Determine probability of compromise
- Perform impact analysis
- Rank risks
- Develop mitigation strategy
- Report findings

Abuse Cases

- Determine:
  - Inputs
  - Activities
  - Outputs
  - Importance
- Create Attack Models
- Create Abuse Cases

Security Requirements

- Security must be explicitly worked into the Requirement, not an afterthought
- Good Security Requirements cover: overt functional security (use of cryptography), and emergent characteristics (from abuse cases and attack patterns)
- Can sometimes be a lengthy process in itself