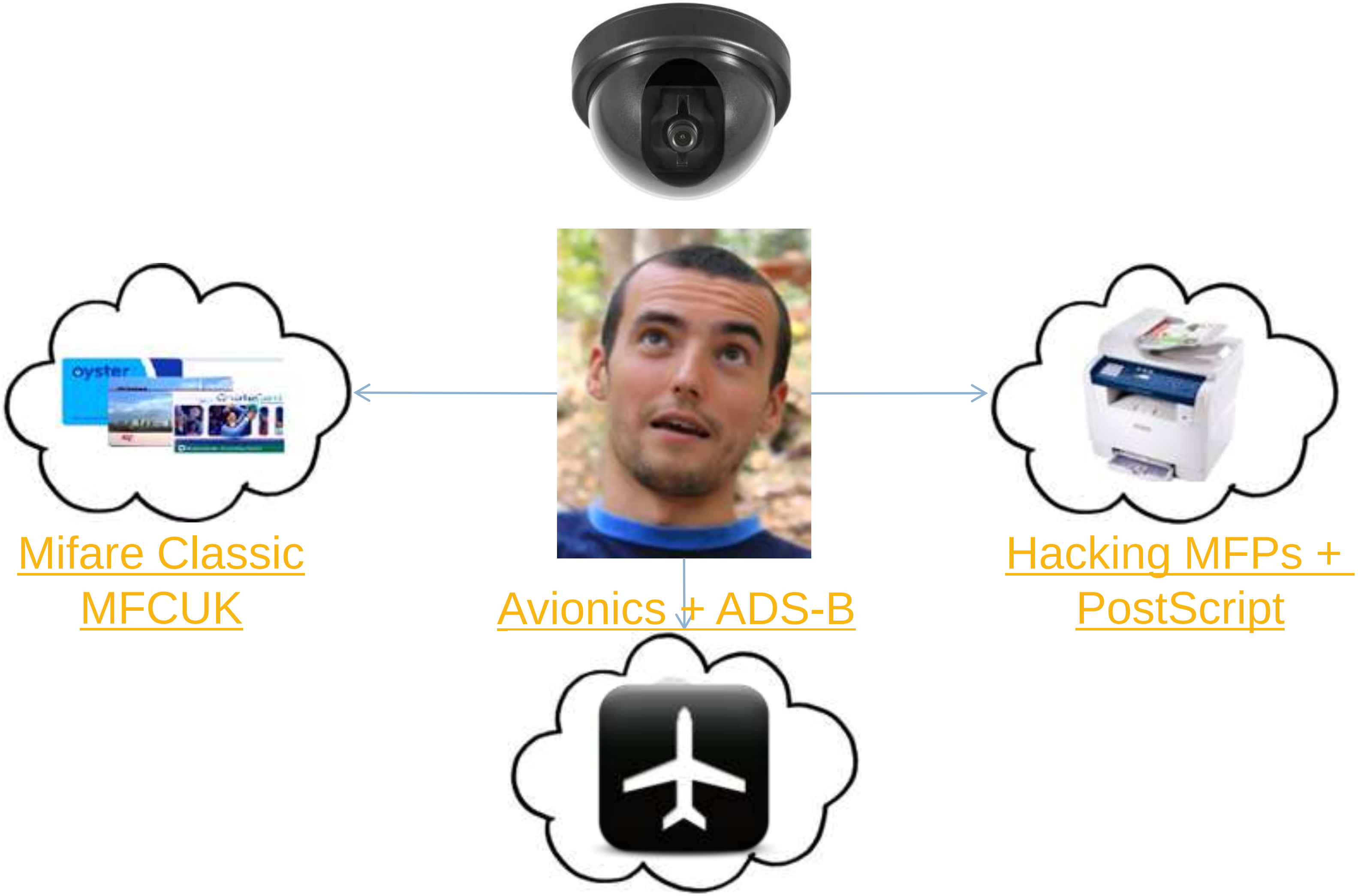
Poor Man’s Panopticon
Mass CCTV Surveillance for the masses

Andrei Costin
@costinandrei
FIRMWARE.RE

andrei# whoami
SW/HW/Emb security researcher, PhD student



Mifare Classic
MFCUK

Avionics + ADS-B

Hacking MFPs +
PostScript

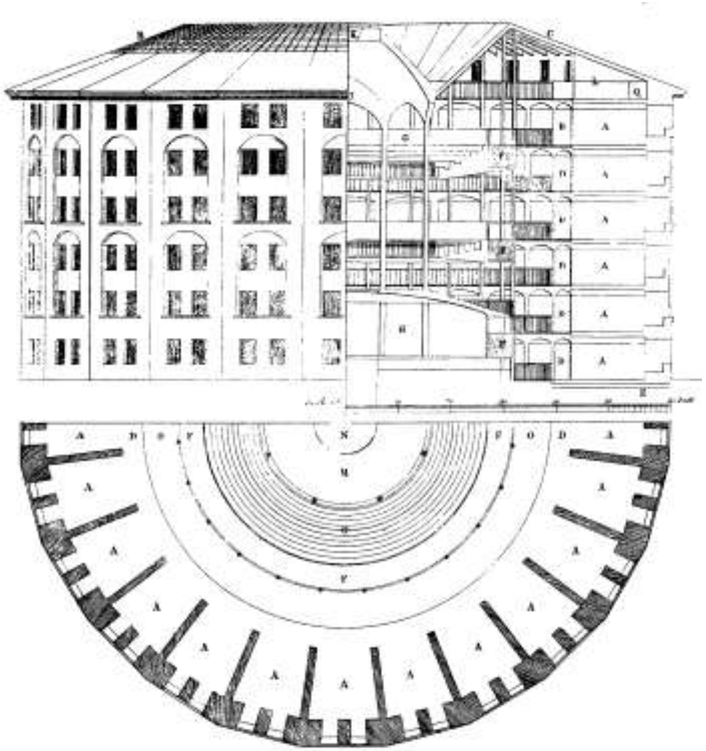
DISCLAIMER

- This presentation is for informational purposes only. Do not apply the material if not explicitly authorized to do so
- Reader takes full responsibility whatsoever of applying or experimenting with presented material
- Authors are fully waived of any claims of direct or indirect damages that might arise from applying the material
- Information herein represents author own views on the matter and does not represent any official position of affiliated body

- **tldr;**
- **DO NOT TRY THIS AT HOME!**
- **USE AT YOUR OWN RISK!**

Intro – Panopticon

- The concept of the design is to allow a watchman to observe (-*opticon*) all (*pan*-) inmates of an institution without them being able to tell whether they are being watched or not
- Synonym for “Big-Brother”



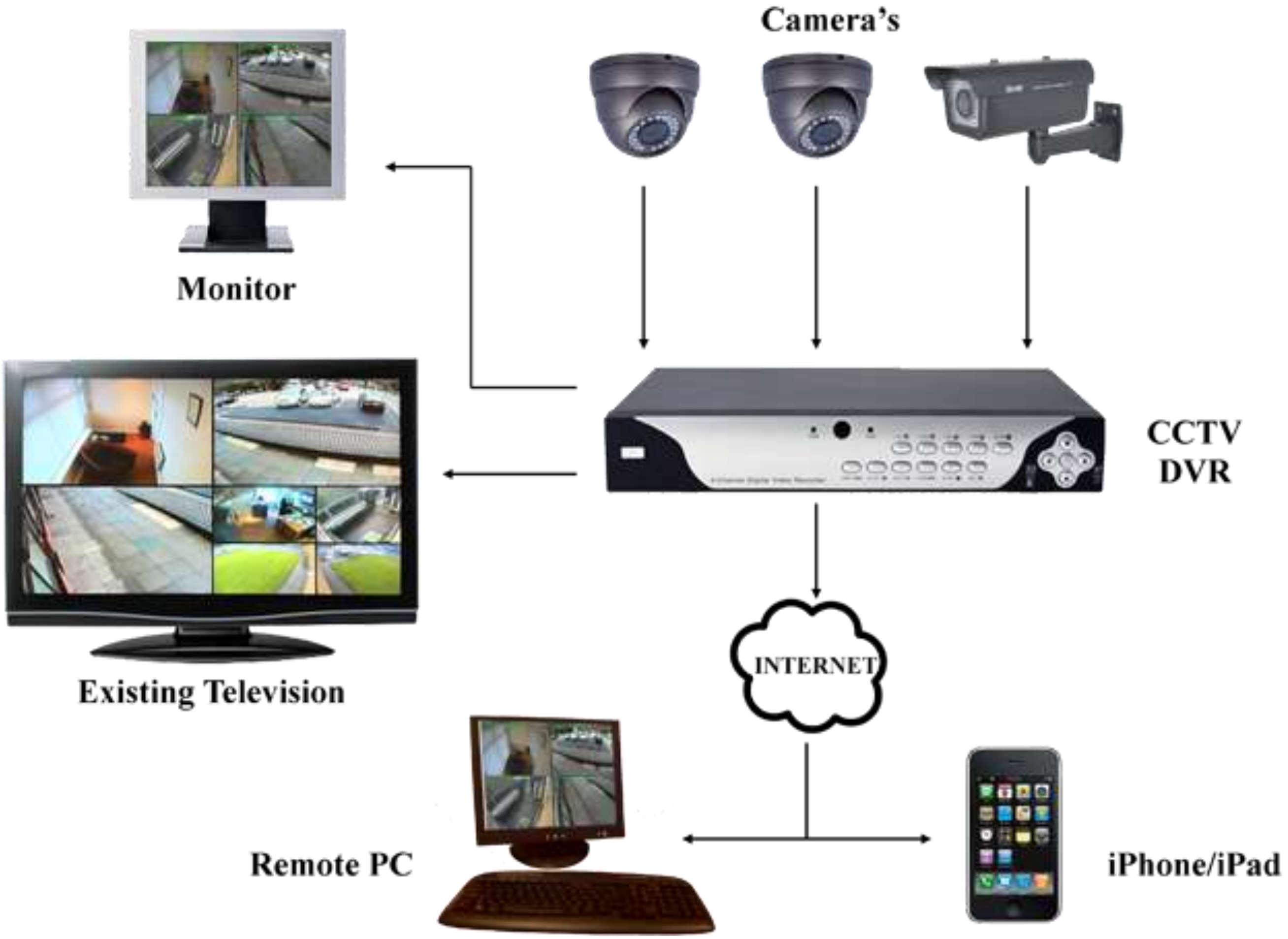
Intro – CCTV

- CCTV as in “Closed Circuit TV”
    - Not as in “CNTV CCTV9 China Central Television”

- Meaning:
    - BNC cameras
    - RF cameras
    - IP cameras
    - DVR/NVR systems
    - And all HW + SW + Analytics + Integration + Interfacing systems

Intro – CCTV

- Simplified schematic of most CCTV systems today:



Timeline – Existing Work

- Early "IP cameras google dorks“
- 2005 22C3 - Hacking CCTV. A private investigation.
- 2007 - ProCheckup - Owning Big Brother: Multiple vulnerabilities on Axis 2100 IP cameras
- 2010 BH10DC - Joshua Marpet - Physical Security in a Networked World: Video Analytics, Video Surveillance, and You

Timeline – Existing Work

- 2011 - DigitalMunition - Owning a Cop Car
- 2012 DefCon - Robert Portvliet and Brad Antoniewicz - The Safety Dance: Wardriving the Public Safety Band.
- 2013 HITB AMS - Sergey Shekyan and Artem Harutyunyan - To Watch Or To Be Watched. Turning your surveillance camera against you.
- 2013 BH13US - Craig Heffner - Exploiting Surveillance Cameras. Like a Hollywood Hacker.

Timeline – In the recent news

- 28 Oct 2013 - "Israeli Road Control System hacked ... seems that the attackers used a malware to hit *the security camera apparatus* in the Carmel Tunnel toll road in Sept. 8 and to gain its control“

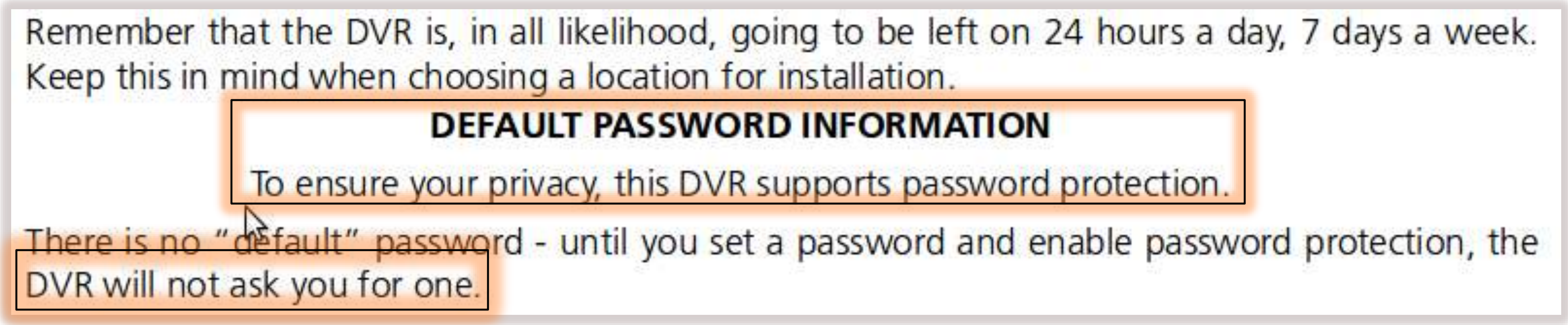
- 4 Sep 2013 – “FTC settles with Trendnet after *'hundreds' of home security cameras* were hacked... FTC Forcing TRENDnet to Suffer 20 Years of Auditing.”

- How about... *hundreds of thousands*?!

Reality Check
The state of security of CCTV products?

- Few roots of most evils: "*Default credentials, design f@$k-ups and dumb users“*"

- Kafkian-style notes in the documentation



Remember that the DVR is, in all likelihood, going to be left on 24 hours a day, 7 days a week. Keep this in mind when choosing a location for installation.

DEFAULT PASSWORD INFORMATION

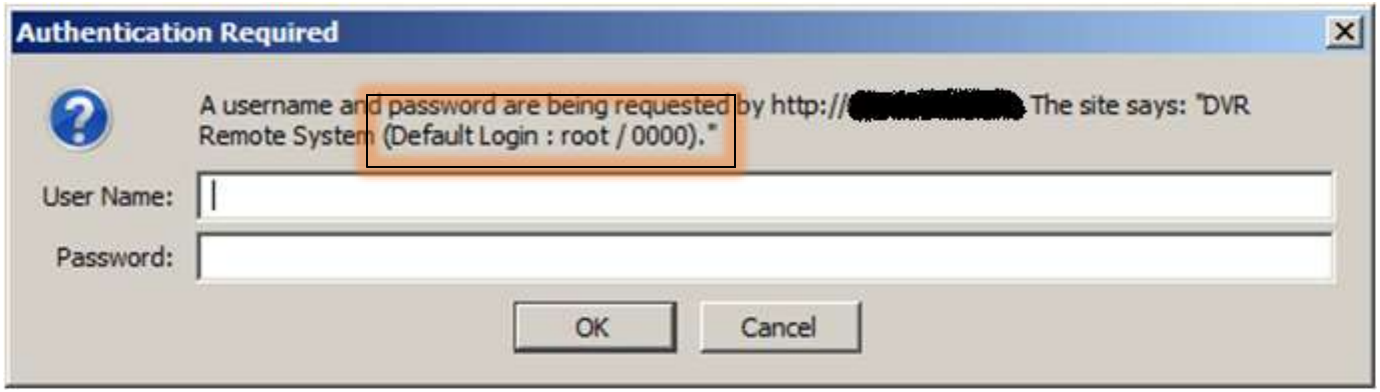
To ensure your privacy, this DVR supports password protection.

There is no “default” password - until you set a password and enable password protection, the DVR will not ask you for one.

Reality Check
The state of security of CCTV products?

- Few roots of most evils: *"Default credentials, design f@$k-ups and dumb users“*

- Insane design and even more insane users
  - Some user leave these on indefinitely…



Authentication Required

A username and password are being requested by http://[redacted] The site says: "DVR Remote System (Default Login : root / 0000)."

User Name:

Password:

CCTV Device Population – Search & Results

- Goal:
  - Estimate publicly accessible IPcam/DVR/NVR/CCTV systems
  - So, how much can someone theoretically own?

- Sources:
  - Shodan
  - Internet Census 2012
  - (optional) Google dorks

- Results:
  - Statistics and queries should be released soon

CCTV Device Population – Search & Results

- Results – Internet Census 2012 (top matches)

TOTAL	~ 450.000	
Avtech AVN801 network camera	137,066	AvTech
GeoVision GeoHttpServer for webcams	121,907	GeoVision
Netwave IP camera http config	53,813	Foscam
DVR Systems webcam http interface	18,775	?
Netwave webcam http config	15,785	Foscam
Swann DVR8-2600 security camera system httpd	15,458	Swann

CCTV Device Population – Search & Results

- Results – Shodan (top matches, Jun 2013)
  - Today – numbers are ~10-20% up

TOTAL	>> 1,200,000	
q=netwave+camera	332,342	Foscam
q=port%3A80+Avtech	309,801	AvTech
q=GeoHttpServer	278,148	GeoVision
q=Server%3A+alphapd	89,831	?
q=realm%3D"DVR"	87,095	Hunt/Svat/Defender
q=Server%3A+Network+Camera	51,378	Mixed
q=dcs-lig-httpd	50,547	D-Link

CCTV Device Population – Fun Facts

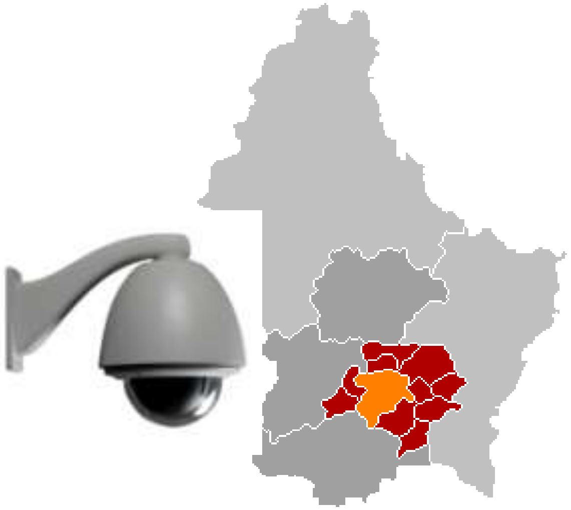
- Let’s map “surveillance” coverage of publicly accessible CCTV device population over a geographical area
    - As if all exposed devices were located in a given area

- Assumptions:
    - between 450k and 1.2M devices, let’s take 500k devices
    - each found "device" covers 100 m2 (10x10m)
    - stretched assumption, but reasonable on average
        - many DVRs with 2 to 32 cameras each
        - many cameras are good resolution HD
    - all devices cover a continuous flat surface/space

CCTV Device Population – Fun Facts

- Math:
  - 500.000 x 100 m2 =
    50.000.000 m2 = 50 km2

- City of Luxembourg ~ 51.46 km2
  - We could survey
  - City of Luxembourg entirely (orange spot)



- Monaco ~ 2.02 km2
  - If Monaco was covered totally by a 25 floor state-wide building
  - We could survey that state-wide building entirely

CCTV Online Live Demo Systems

- What?
  - IPcam/DVR/CCTV systems put intentionally on the internet by the vendor or security/surveillance online shops

- Why?
  - Usual audience – Intended for marketing and sales boost
  - Geek audience – think differently ☺

- How?
  - Google for:
  - "demo dvr”, "demo nvr”, "cctv demo“
  - "live cctv demo”, "live dvr"

CCTV Online Live Demo Systems

- Google dork stopped working? Let's create our own brand new!

Targets and Motivations

- Attackers by motivation
  - Voyeurs, Stalkers, Criminals, Govt Organizations, Hacktivism Groups
- Targets
  - Persons, Cars, Property
  - Embedded devices
    - PCs of operators (secondary)
    - Other integrated interfaces (see Israeli's road control sys)

Targets and Motivations

- Motivations
  - Money (eg.: blackmailers, bounty hunters for fugitives/missing-persons/stolen-cars)
  - Covering a crime (eg.: robbery – tap-in before, DoS during, restore after)
  - Uncovering cenzorship (eg.: hacktivism – checking what is going on for real during demonstrations)
  - Botnets of embedded devices

Attacks – Types by Location

- Remote
  - may come as a remote scan & exploit (classical)

- Local (Software)
  - may come as local-network exploit (classical)
  - may come as a physical attack over USB

- Local Physical Proximity
  - may come as a physical attack over infra-red
  - may come as a physical attack over USB
  - may come as a software attack over "visual layer"

Attacks – Unconventional – Invisible layer

- Infra-red channel – DoS, Command injection

Out of service

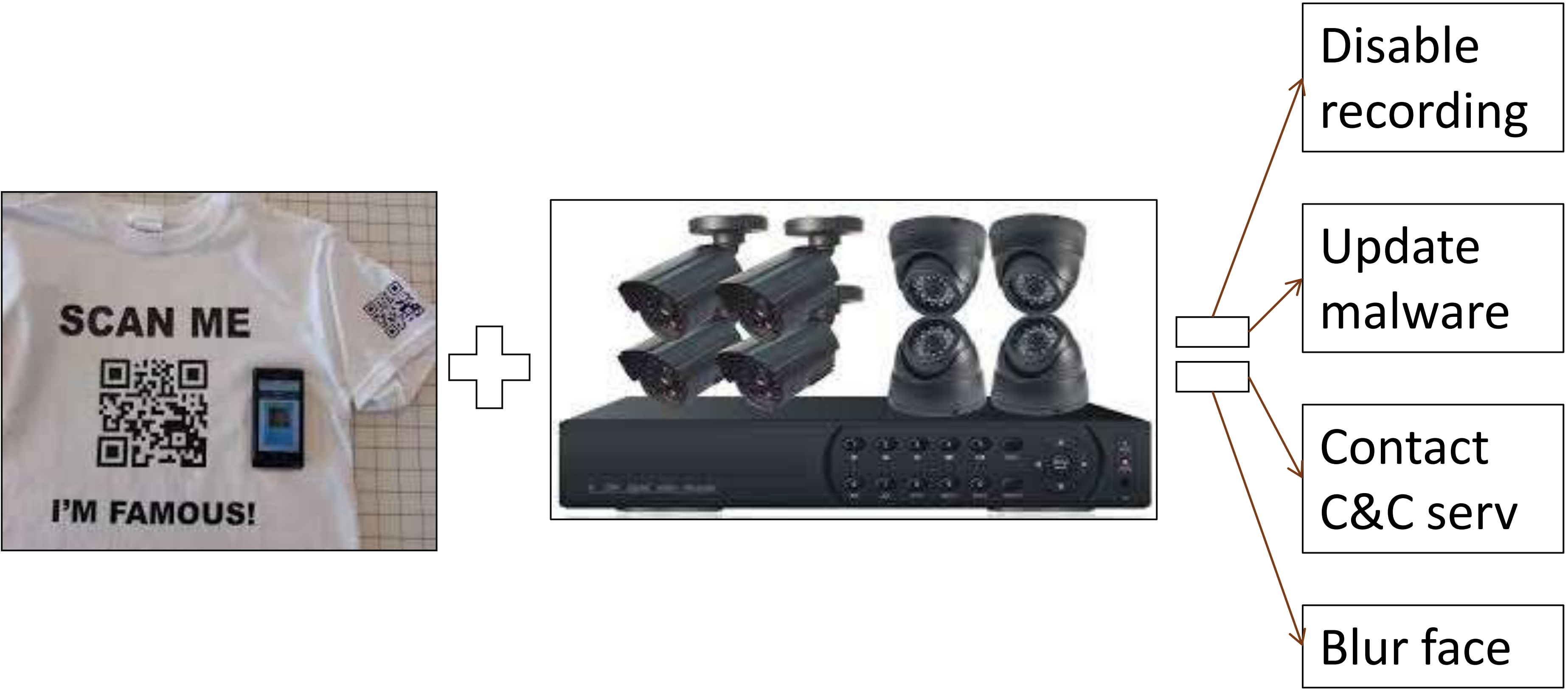
Attacks – Unconventional – Visual layer

- *Visual layer backdoors (more wicked than Google Glass hack)*
- Visually encoded information
  - QR codes
  - Any other visual (custom) code that can convey info & commands
  - Can be as custom as a

- The trick is to highly-reliable trigger
  - accurate visual mark detection
  - accurate decoding visually-encoded info & commands

Attacks – Unconventional – Visual layer

- Visually encoded information and commands example



Disable recording

Update malware

Contact C&C serv

Blur face

Attacks – Unconventional – Visual layer – How?

- *Software* (video I/O kernel modules, streaming application video filters)
  - easy to hard to detect or reverse

- *Hardware* (integrated video/audio codecs and chipsets)
  - hard to impossible to detect or reverse
  - even if I/O to chip is possible

- The range of video imagery pixels to create a “semantic” image is huge
  - hard to trigger, thus detect, "visual information decoding" after all

Attacks – Most Common Vulnerabilities

- Backdoor credentials/access

Attacks – Most Common Vulnerabilities

- Clear-text credential storage + Insufficient access controls

Attacks – Most Common Vulnerabilities

- Old software (kernel, web-server, interpreter)

Attacks – Most Common Vulnerabilities

- Denial of Service
    - DoS on CCTV is critical, not a nuisscance
    - Weakest points seem to be /cgi-bin/*
        - Causing coredump & reboots
    - Short demo

- Rogue/Modified firmware
    - Short demo

- Command-injection
    - Eg: via ping *"127.0.0.1; evil_command_here;“*

- Insufficient access controls on webroot and filesystem

I pwn device(s). Now what?

- Determining geo-location can be
  - Useful, eg. for finding missing persons, stolen car
  - Dangerous, eg. for tracking people

- Getting video stream is really useful, but how?
  - iSpyConnect – APIs and software
  - Detect camera vendor, grab the API and off you go

- What about faces?
  - Face detection and recognition is easy these days
  - OpenCV is our friend

I pwn the device. Now what?

- Demo

Closing thoughts

- Hitachi Hokusai Electric CCTV Camera
  - Can Scan 36 Million Faces/Second

- LG Roboking VR680VMNC equipped with wi-fi and
  - 3 cameras at once to capture the surrounding areas

- What’s next?

Summary

- Around 1,000,000 publicly exposed DVRs/IPCAMs/CCTVs
- Demonstrated multiple attacks
- Demonstrated new vulnerabilities
- Introduced novel attack ideas
- DVR/IPCAM/CCTV vendors must secure their systems better

Thank you!
Questions, ideas, corrections?

zveriu@gmail.com
http://andreicostin.com/papers/
http://andreicostin.com/secadv/