What the Watchers See

Weaknesses in Municipal Mesh Network Deployments

Dustin Hoffman & Thomas (TK) Kinsey
DEF CON 22
Dustin Hoffman
the researcher, not the actor :’(  

- Senior Engineer @ Exigent Systems
- Principal @ various other concerns
Thomas (TK) Kinsey

- Senior Engineer @ Exigent Systems
- Principal @ 3Kappa Research
What The Watchers See

How it started

... open wifi network(s) available
What The Watchers See

The Transparent Society by David Brin

What The Watchers See

Why are municipalities deploying these networks?

City services: police, traffic, 2-way audio, site monitoring, force multiplier, shrinking budgets :(

exigent systems
What The Watchers See

Network implementation

Wireless mesh

Motivations: lower cost, shorten install time, no trenching, permitting
What The Watchers See

Project / Integration Vendors

E.g., LeverageIS

http://www.leverageis.com/
What The Watchers See

Real-Time Response to Real-Time Crime

Leverage our expertise in technology - and put it to work for you

LEVERAGE is focused on providing its customers with an intelligent and unified approach to solving their business problems. The results of this work are tightly integrated IT and business solutions that meet the customer’s critical requirements.
What The Watchers See

Implementation Hardware

Common off-the-shelf hardware
e.g. Firetide/UNICOM, Bosh cameras, DVR/NVRs
What The Watchers See

Our Lab

[Image of a device with cables on the floor]

[Image of another device with cables on the floor]
What The Watchers See


[Exigent Systems logo]
What The Watchers See

Firetide specific info:
filesystem
reverse engineering
etc.
What The Watchers See

Implementation Protocols

802.11 2.4Ghz, 5Ghz, & 900Mhz

Mesh: Open standards vs AutoMesh

Interestingly, 2.4Ghz is in use, not mentioned

What The Watchers See

Mesh in general:

• Multiple wireless paths
• Nodes aren’t guaranteed a reliable connection to the backhaul
• Protocol provides node IDs, mesh health info, etc.
What The Watchers See

Wired

Mesh
What The Watchers See

Mesh in Our Specific Case

What The Watchers See

AutoMesh Specifics

• Proprietary & details not published
• 19 patents to date
What The Watchers See

AutoMesh Specifics

External headers look normal
What The Watchers See

AutoMesh Specifics

Header part 1 of 2
What The Watchers See

AutoMesh Specifics

Header part 1 of 2 (broadcast)
What The Watchers See

AutoMesh Specifics

Header part 2 of 2 (broadcast again)
What The Watchers See

AutoMesh Specifics
Enclosed header looks normal

This one’s a CDP packet.
What The Watchers See

Specific case

https://mapsengine.google.com/map/edit?mid=zLPNQgdI24w4.kIDGLs4MNR3w

Open before, now with WEP!!
What The Watchers See

Specific case


http://www.cityofredlands.org/sites/default/files/pdfs/Under_the_Watchful_Eye.pdf


What The Watchers See
What The Watchers See
What The Watchers See
What The Watchers See
What The Watchers See
What The Watchers See
What The Watchers See

This sign makes it all OK....
What The Watchers See

Security

- Access to transmission medium
- node authentication (bank calling/GSM)
- link encryption
What The Watchers See

Security

- Direction antennae to “secure” medium
What The Watchers See

Security

- Content encryption
- Node authentication via PKI, not turned on
- AutoMesh as security / obscuration
What The Watchers See

Security

- Sloppy integrators
- No in-house expertise or on-going testing / pen-testing, ‘cuz $$$
What The Watchers See

Potential Threats

• !! Federal & State wiretapping laws, or more, may be applicable in your research. Please contact a legal professional
• IANAL
• info@eff.org
What The Watchers See

Potential Threats

• Observing video streams
• Multicast: subscribe yourself to arbitrary feeds
What The Watchers See

Potential Threats

Denial of service via:

- flood
- crude jamming
- oversubscribe
What The Watchers See

Potential Threats

• ARP spoof: become a node or the NVR/DVR

... so dirty.
What The Watchers See

Potential Threats

Or easier:

• Join the mesh “legitimately”
• There are only 256 “mesh IDs”

... so dirtier.
What The Watchers See

Potential Threats

• Access to internal municipal network / PD
What The Watchers See

Potential Threats

- Video manipulation/injection “all’s well”
What The Watchers See

Potential Threats

- UDP increment attack
What The Watchers See

UDP increment attack (1)
What The Watchers See
UDP increment attack (2)
What The Watchers See

UDP increment attack (3)
What The Watchers See

UDP increment attack (4)
What The Watchers See

Potential Threats

• Non-video manipulation: infrared tripwires & area sensors to direct police resource or draw attention
What The Watchers See

Privacy Abuse & Misuse

• Long-term Archival
• General shenanigans (VZ tech, NSA 20 yr olds)
What The Watchers See

Demo is Sad ‘cuz WEP 😞
What The Watchers See

THANK YOU!