

# 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

[http://archive.wired.com/wired/archive/4.12/fftransparent\\_pr.html](http://archive.wired.com/wired/archive/4.12/fftransparent_pr.html)

# What The Watchers See

Why are municipalities deploying these networks?

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

# 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

The screenshot shows the LEVERAGE INFORMATION SYSTEMS website. At the top left is the company logo. To the right is a search bar with a magnifying glass icon. Below the logo is a navigation menu with links for Home, About, Solutions, Services & Support, Products & Technology, Contracts, News, and Contact. The main content area features a large image of a woman in profile, looking at a mobile device. Overlaid on the image is the text "Real-Time Response to Real-Time Crime" and a "Learn More>>>" button. Below the image are "Previous" and "Next" navigation arrows. Underneath the image is a sub-header: "Leverage our expertise in technology - and put it to work for you". This is followed by a paragraph: "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". At the bottom, there are four content blocks: "LEVERAGE Tech Blog" with a login form image, "Technology Partners" with a Cisco Partner Gold Certified logo and a gold star, "School Security & Safety" with a school building image, and "News" with a person's face image.

**LEVERAGE**  
INFORMATION SYSTEMS

Search

Home | About | Solutions | Services & Support | Products & Technology | Contracts | News | Contact

Real-Time Response  
to Real-Time Crime

Learn More>>>

Previous Next

**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

LEVERAGE Tech Blog

Technology Partners

School Security & Safety

News

# 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



# What The Watchers See









firetide All Categories


Related: mimo antenna 5ghz antenna raymarine hsb2 raymarine hsb ellusionist playing cards hotpoint lucille ball fireside cisco 2...

All Listings Auction Buy It Now Sort: Best Match View: [grid]

30 results for firetide [Follow this search](#)

Did you mean: [fireside?](#) (7,032 items)

 2 Photos	Firetide Hotport 6100 Indoor Mesh Node	2d 18h left Saturday, 1PM	<b>\$119.99</b> 0 bids
	Firetide - 3000-9000-ELE-1 - Hotview Pro Mesh Management Software (electronic)		<b>\$149.76</b> Buy It Now
 4 Photos	BRAND NEW Firetide HotPoint 4200 Wireless Access Point. Outdoor Rated	 FAST 'N FREE - Get it on or before Tue, Aug. 12	<b>\$99.99</b> or Best Offer Free shipping
 5 Photos	FireTide Hotport Wireless Mesh Node 3100 / PS	 Top Rated Plus  FAST 'N FREE - Get it on or before Tue, Aug. 12	<b>\$99.99</b> or Best Offer Free shipping
	FIRETIDE SW-7000-RADIO-1 7000 SERIES RADIO LIC		<b>\$458.00</b> Buy It Now

 Reliable connectivity anywhere™

# 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

<http://www.cityofredlands.org/sites/default/files/Purchasing/Public%20Safety%20Camera%20System%20Admin%202014%20RFP%205.5.14.pdf>

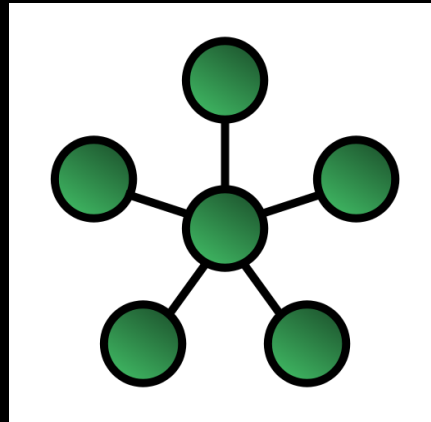
# What The Watchers See

## Mesh in general:

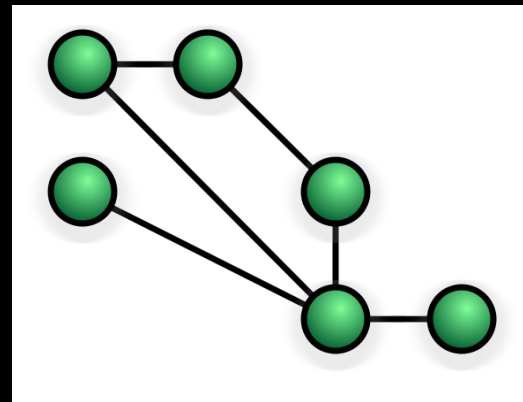
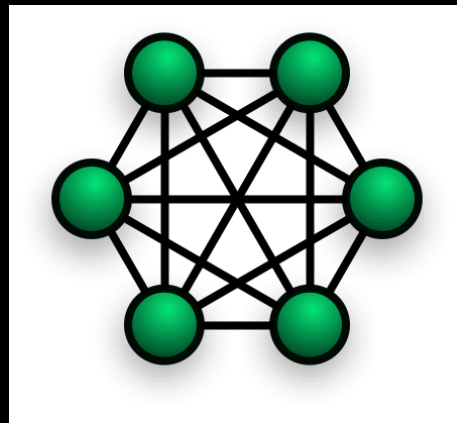
- Multiple wireless paths
- Nodes aren't guaranteed a reliable connection to the backhaul
- Protocol provides node IDs, mesh health info, etc.

# What The Watchers See

Wired



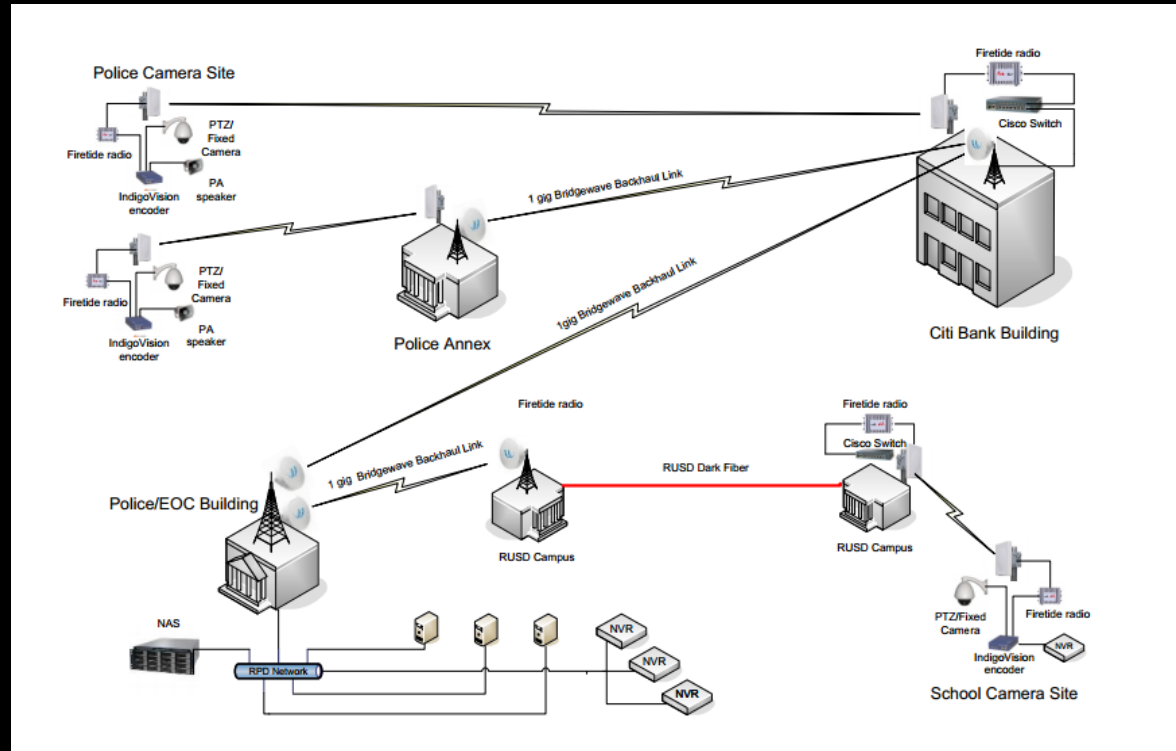
Mesh





# What The Watchers See

## Mesh in Our Specific Case



<http://www.cityofredlands.org/sites/default/files/Purchasing/Public%20Safety%20Camera%20System%20Ad>

# What The Watchers See

## AutoMesh Specifics

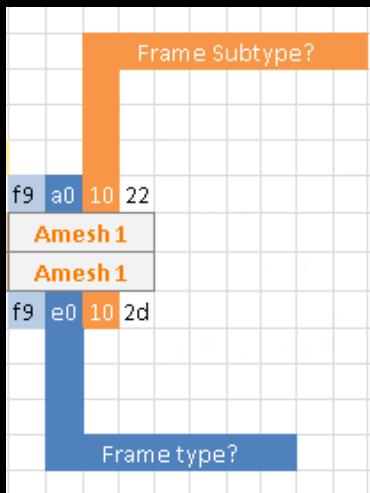
- Proprietary & details not published
- 19 patents to date



# What The Watchers See

## AutoMesh Specifics

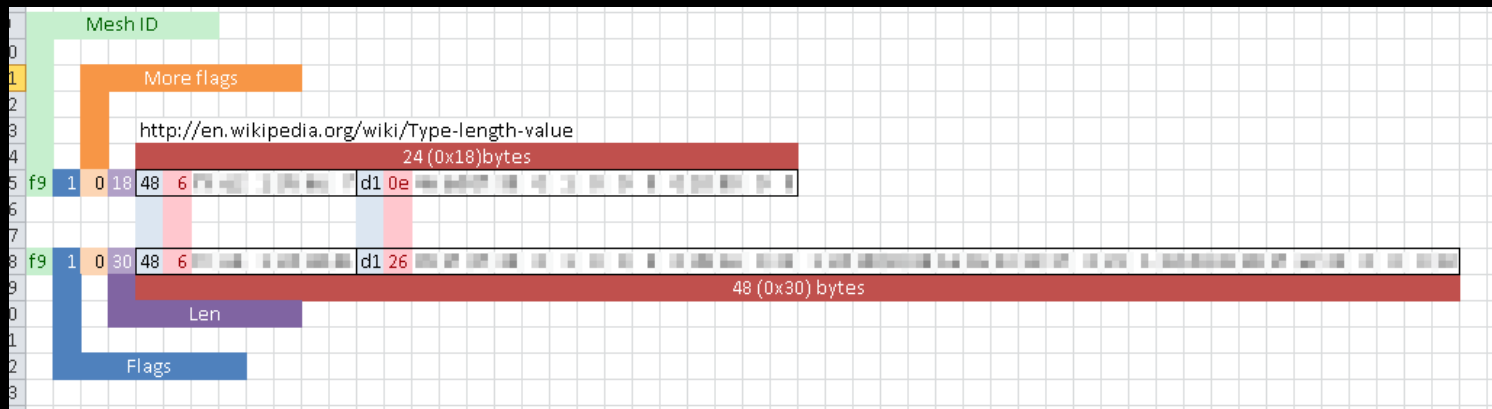
### Header part 1 of 2



# What The Watchers See

## AutoMesh Specifics

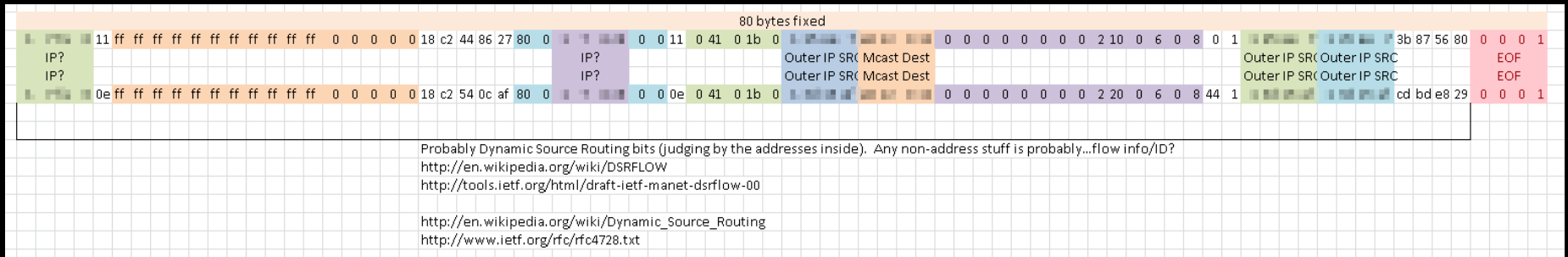
### Header part 1 of 2 (broadcast)



# What The Watchers See

## AutoMesh Specifics

### Header part 2 of 2 (broadcast again)



# What The Watchers See

## AutoMesh Specifics

Enclosed header looks normal

Encapped Header				
DST MAC	SRC MAC	VLAN 1	LEN	LLC, type CDP
DST MAC	SRC MAC	VLAN 0	LEN	LLC, type CDP

This one's a CDP packet.

# What The Watchers See

Specific case



<https://mapsengine.google.com/map/edit?mid=zLPNQgdIZ4w4.kIDGLs4MNR3w>

Open before, now with WEP!!



# What The Watchers See

## Specific case

<http://www.cityofredlands.org/sites/default/files/Purchasing/Public%20Safety%20Camera%20System%20Admin%202014%20RFP%205.5.14.pdf>

[http://www.cityofredlands.org/sites/default/files/pdfs/Under the Watchful Eye.pdf](http://www.cityofredlands.org/sites/default/files/pdfs/Under%20the%20Watchful%20Eye.pdf)

[http://www.cityofredlands.org/sites/default/files/pdfs/Video surveillance guidelines.pdf](http://www.cityofredlands.org/sites/default/files/pdfs/Video%20surveillance%20guidelines.pdf)

<http://www.leverageis.com/pdfs/Yucaipa%20to%20install%20city-wide.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](mailto: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.

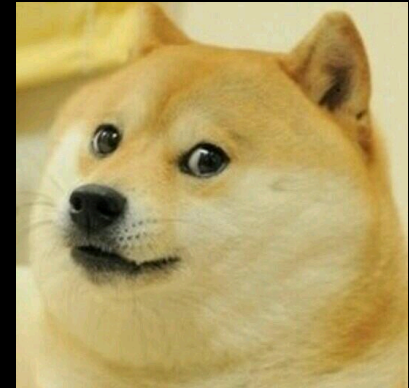


# What The Watchers See

## 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”

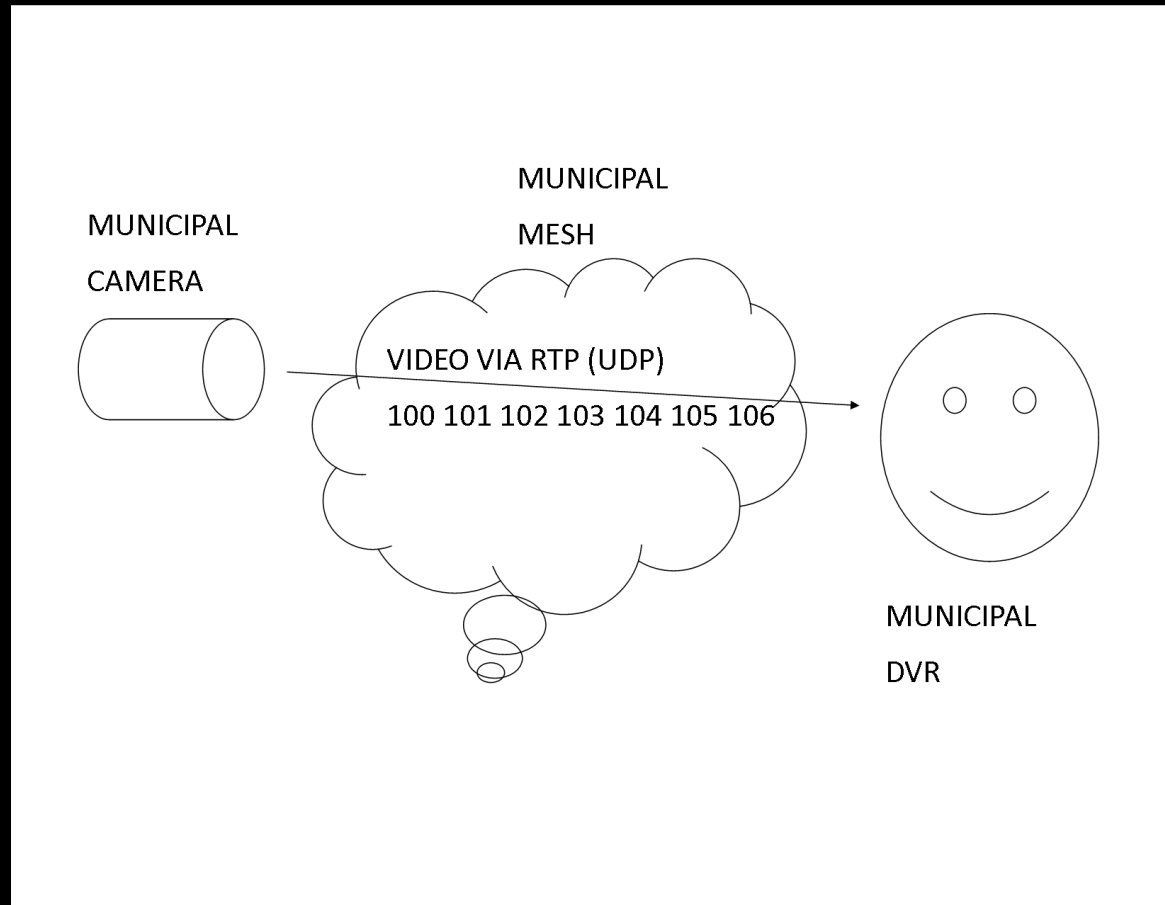
# What The Watchers See

## Potential Threats

- UDP increment attack

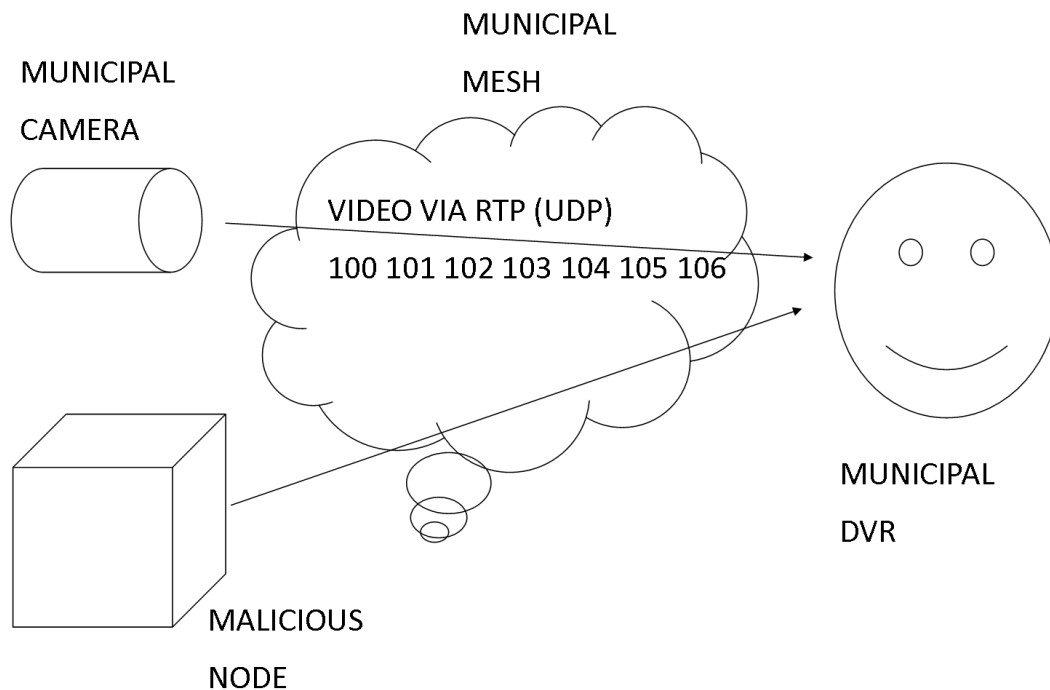
# What The Watchers See

## UDP increment attack (1)



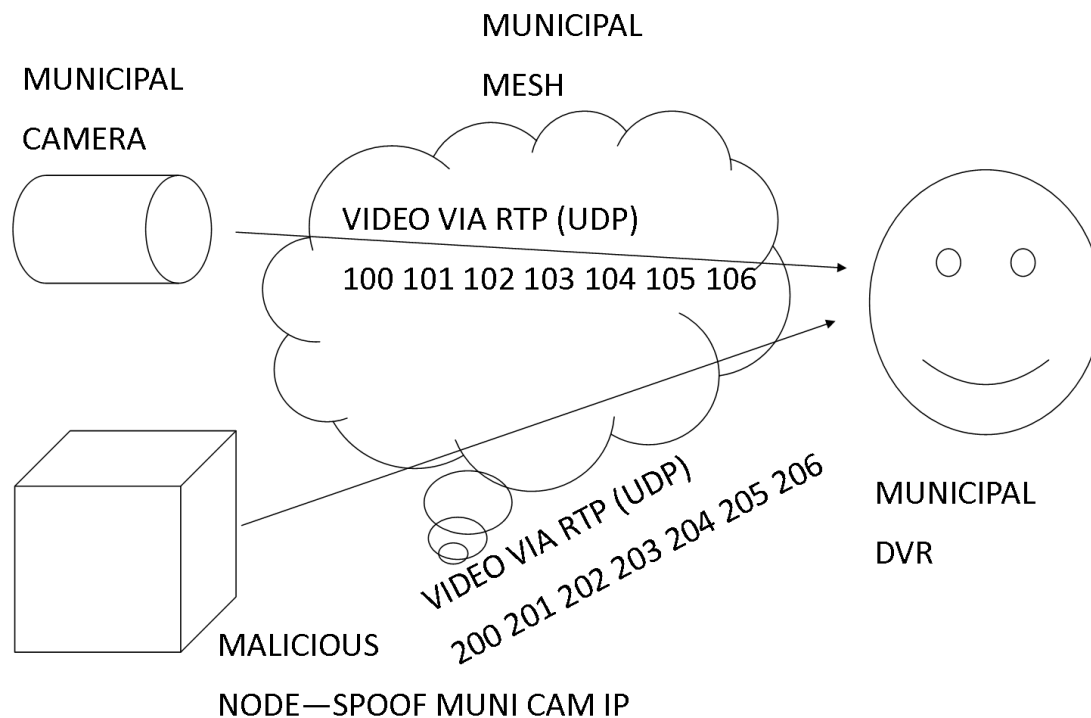
# What The Watchers See

## UDP increment attack (2)



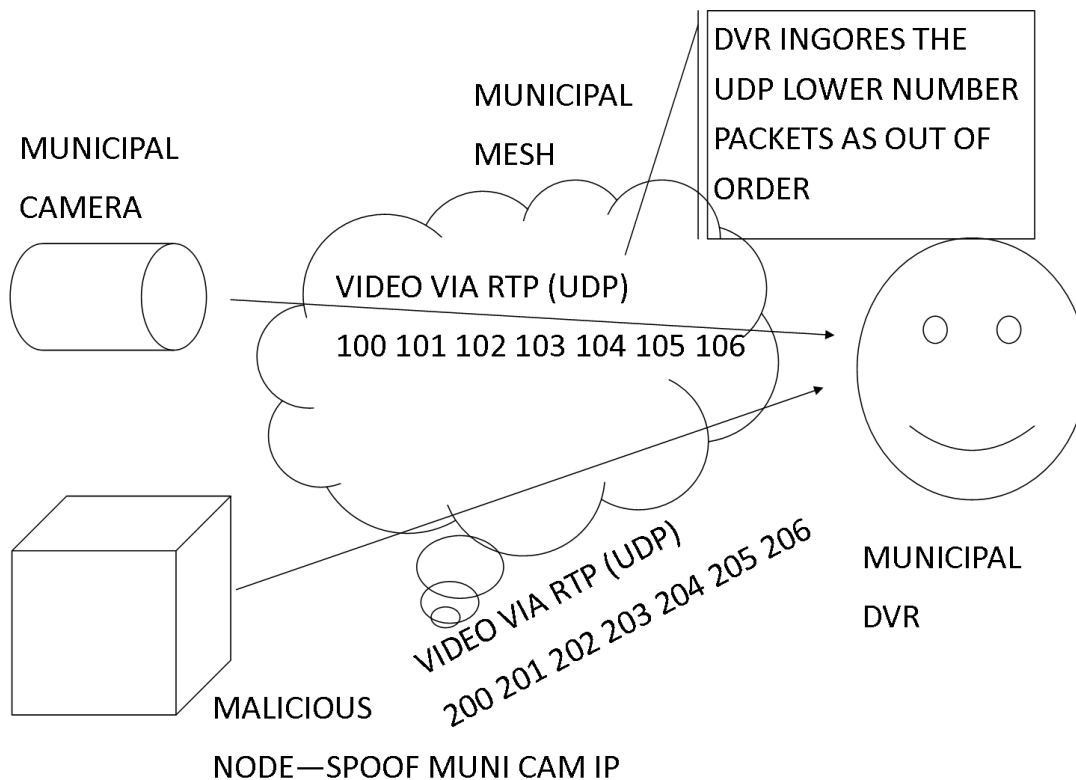
# What The Watchers See

## 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!

