Dartmouth Internet Security Testbed (DIST): building a campus-wide wireless testbed

Sergey Bratus David Kotz Keren Tan William Taylor
Anna Shubina Bennet Vance[1]
Michael E. Locasto[2]

[1]Dartmouth College, Hanover, New Hampshire

[2]George Mason University, Fairfax, Virginia

2nd Workshop on Cyber Security Experimentation and Test, 2009

Outline

Outline

DIST Architecture and Operation

Covered in this talk: Dartmouth Internet Security Testbed (wireless)

DIST wireless in short

- Over 200 wireless Air Monitors capturing 802.11 frames
  - Aruba AP70 access points reflashed with OpenWRT firmware
- DIST servers processing the captured frames and storing sanitized data
- Launchpad, a DIST server that alone may launch experiments using the Air Monitors

DIST Architecture and Operation

Covered in this talk: Dartmouth Internet Security Testbed (wireless)

DIST wireless in short

- Over 200 wireless Air Monitors capturing 802.11 frames
  - Aruba AP70 access points reflashed with OpenWRT firmware
- DIST servers processing the captured frames and storing sanitized data
- Launchpad, a DIST server that alone may launch experiments using the Air Monitors

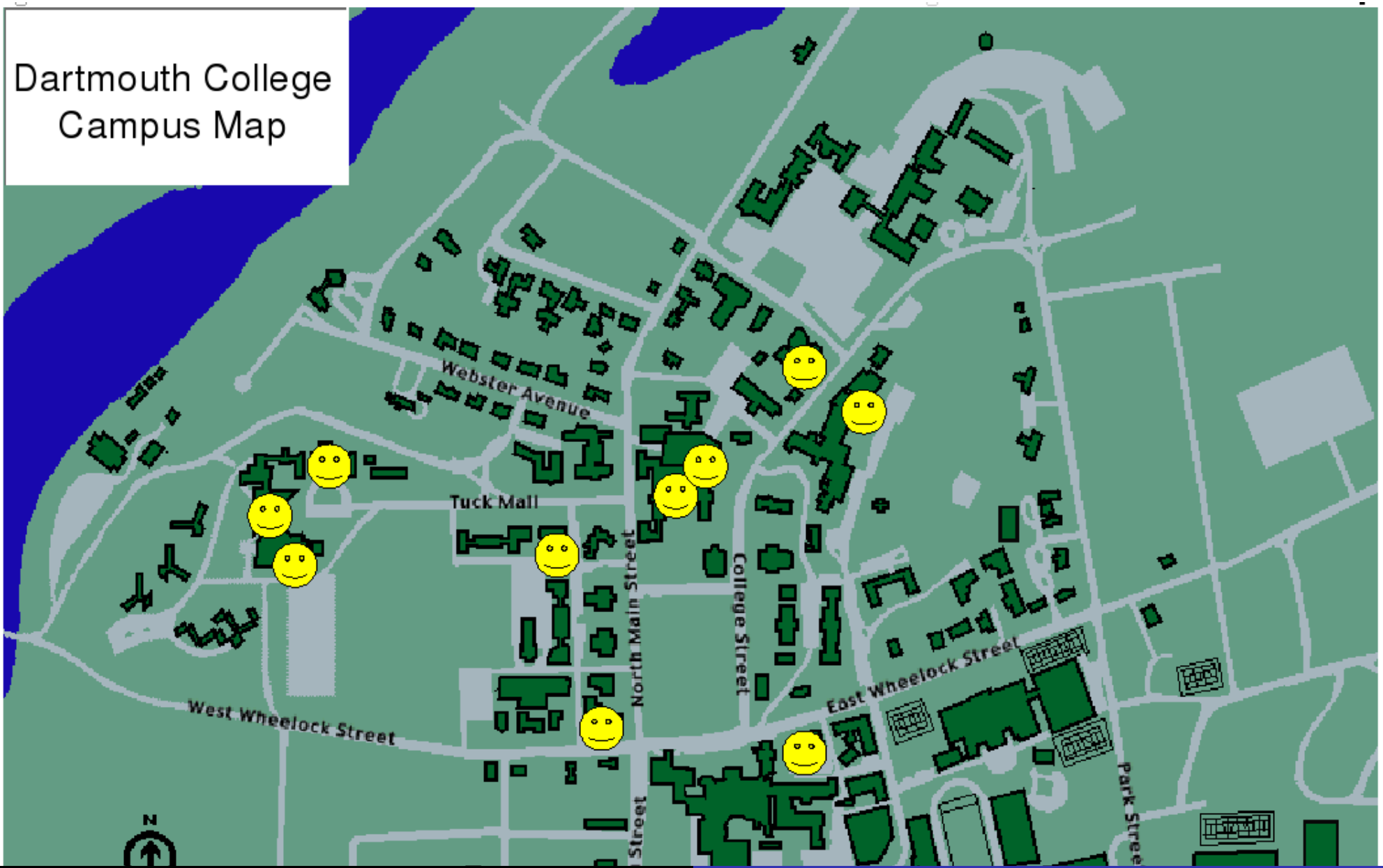
DIST Architecture and Operation

Covered in this talk: Dartmouth Internet Security Testbed (wireless)

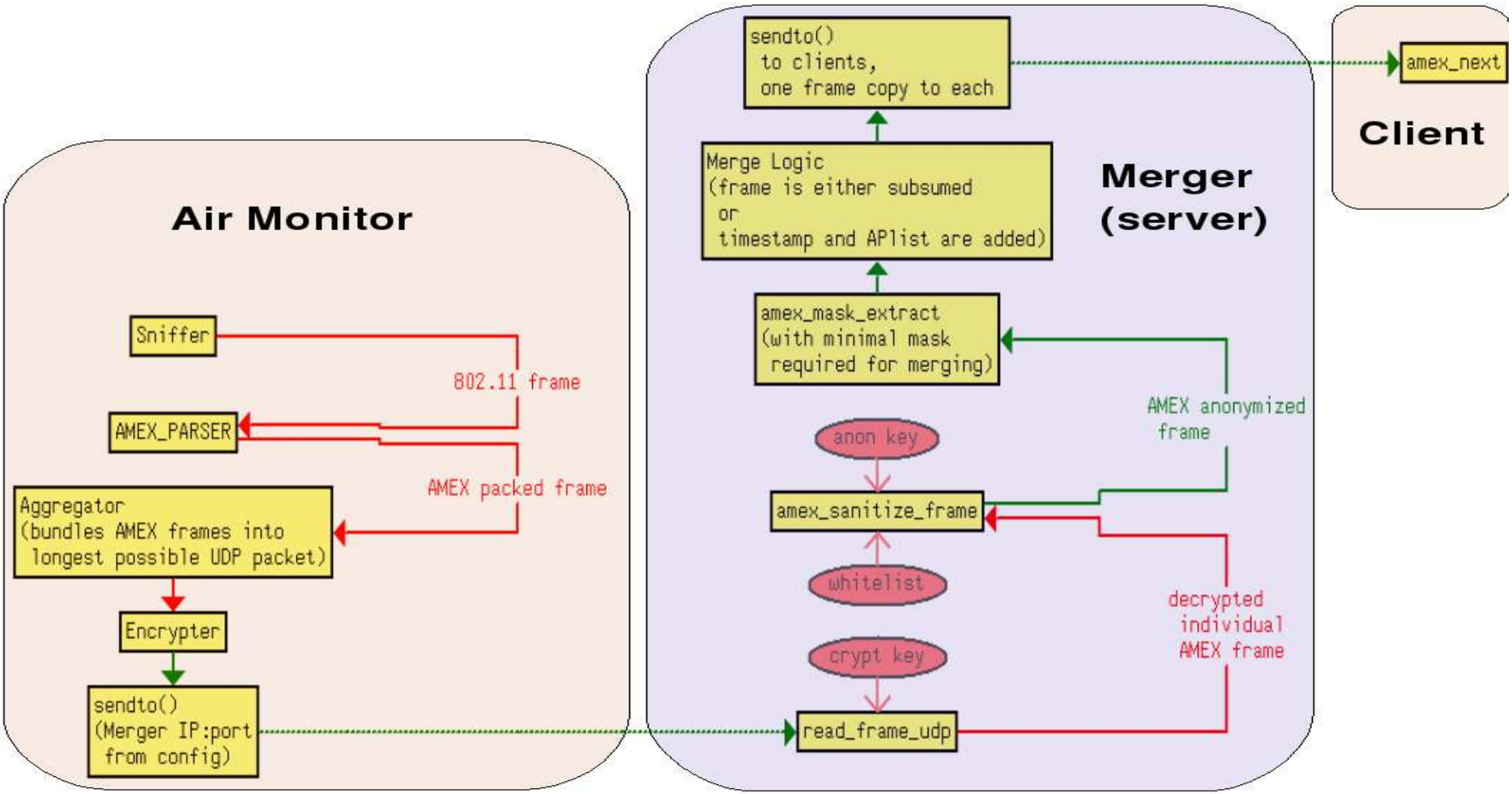
DIST wireless in short

- Over 200 wireless Air Monitors capturing 802.11 frames
  - Aruba AP70 access points reflashed with OpenWRT firmware
- DIST servers processing the captured frames and storing sanitized data
- Launchpad, a DIST server that alone may launch experiments using the Air Monitors

DIST at a glance



DIST Architecture and Operation



Red arrows show sensitive traffic. Green arrows show frames that are encrypted or sanitized.

Outline

Data Protection and Sanitization

Why?

"Human layers of the OSI networking model"

- We discard all but the MAC layer.
- We encrypt every packet before sending it to the server.
- The server sanitizes every 802.11 frame header just after decryption.
- Sanitization key is generated anew for every experiment, using a random seed, which is discarded after use.

Why sanitize on the server, not on the AMs?

- Sanitization on AMs would be too CPU-intensive.
- Sharing the sanitization key securely is hard.

Data Protection and Sanitization

Why?

"Human layers of the OSI networking model"

- We discard all but the MAC layer.
- We encrypt every packet before sending it to the server.
- The server sanitizes every 802.11 frame header just after decryption.
- Sanitization key is generated anew for every experiment, using a random seed, which is discarded after use.

Why sanitize on the server, not on the AMs?

- Sanitization on AMs would be too CPU-intensive.
- Sharing the sanitization key securely is hard.

Data Protection and Sanitization

Why?

"Human layers of the OSI networking model"

- We discard all but the MAC layer.
- We encrypt every packet before sending it to the server.
- The server sanitizes every 802.11 frame header just after decryption.
- Sanitization key is generated anew for every experiment, using a random seed, which is discarded after use.

Why sanitize on the server, not on the AMs?

- Sanitization on AMs would be too CPU-intensive.
- Sharing the sanitization key securely is hard.

Data Protection and Sanitization

Why?

"Human layers of the OSI networking model"

- We discard all but the MAC layer.
- We encrypt every packet before sending it to the server.
- The server sanitizes every 802.11 frame header just after decryption.
- Sanitization key is generated anew for every experiment, using a random seed, which is discarded after use.

Why sanitize on the server, not on the AMs?

- Sanitization on AMs would be too CPU-intensive.
- Sharing the sanitization key securely is hard.

Data Protection and Sanitization

Why?

"Human layers of the OSI networking model"

- We discard all but the MAC layer.
- We encrypt every packet before sending it to the server.
- The server sanitizes every 802.11 frame header just after decryption.
- Sanitization key is generated anew for every experiment, using a random seed, which is discarded after use.

Why sanitize on the server, not on the AMs?

- Sanitization on AMs would be too CPU-intensive.
- Sharing the sanitization key securely is hard.

Encryption

Task

Encrypting a continuous stream of frames.

Cipher

Stream cipher Rabbit, optimized for the MIPS 4Kc processor.

- Stream ciphers vs block ciphers.
  - A block cipher is easier to attack by enumerating inputs. (This could be fatal for DIST's easily predictable data)
  - A stream cipher might be faster.
- Rabbit won on AP70s over other eStream ciphers and SNOW2. (Perhaps due to optimized implementation.)

Encryption

Task

Encrypting a continuous stream of frames.

Cipher

Stream cipher Rabbit, optimized for the MIPS 4Kc processor.

- Stream ciphers vs block ciphers.
  - A block cipher is easier to attack by enumerating inputs. (This could be fatal for DIST's easily predictable data)
  - A stream cipher might be faster.
- Rabbit won on AP70s over other eStream ciphers and SNOW2. (Perhaps due to optimized implementation.)

Encryption

Task

Encrypting a continuous stream of frames.

Cipher

Stream cipher Rabbit, optimized for the MIPS 4Kc processor.

- Stream ciphers vs block ciphers.
  - A block cipher is easier to attack by enumerating inputs. (This could be fatal for DIST's easily predictable data)
  - A stream cipher might be faster.
- Rabbit won on AP70s over other eStream ciphers and SNOW2. (Perhaps due to optimized implementation.)

Encryption

Task

Encrypting a continuous stream of frames.

Cipher

Stream cipher Rabbit, optimized for the MIPS 4Kc processor.

- Stream ciphers vs block ciphers.
  - A block cipher is easier to attack by enumerating inputs. (This could be fatal for DIST's easily predictable data)
  - A stream cipher might be faster.
- Rabbit won on AP70s over other eStream ciphers and SNOW2. (Perhaps due to optimized implementation.)

Effects of Compression

Task:

Optimize the Air Monitors' end-to-end throughput.

Encryption + UDP forwarding

6.2–6.4 seconds for 5000 14K jumbo frames (each tens to hundreds of Radiotap and IEEE 802.11 headers).

Compression + encryption + UDP forwarding

5.3–5.4 seconds for the same. The bandwidth is reduced by nearly 80%.

Sanitization

MAC addresses

MAC addresses are not personally identifiable information by itself, but may become such if correlated with other data.

- DIST servers sanitize MAC addresses.
- In transit, MAC addresses are protected by encryption.
- Sanitization key generates pseudo-random numbers and exists only for the time of the process.

ESSIDs

802.11 probe requests are a known privacy risk.

- The last known network's probed ESSID may contain private information, such as the network owner's name.
- DIST sanitizes ESSIDs that are not on Dartmouth whitelist.

Sanitization

MAC addresses

MAC addresses are not personally identifiable information by itself, but may become such if correlated with other data.

- DIST servers sanitize MAC addresses.
- In transit, MAC addresses are protected by encryption.
- Sanitization key generates pseudo-random numbers and exists only for the time of the process.

ESSIDs

802.11 probe requests are a known privacy risk.

- The last known network's probed ESSID may contain private information, such as the network owner's name.
- DIST sanitizes ESSIDs that are not on Dartmouth whitelist.

Outline

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Harsh Realities

- Convincing organizations
  - IT services permissions
  - Risks of research involving human subjects, as seen by Institutional Review Board
  - Convincing the College
- Convincing humans
  - Privacy perceptions
  - Aesthetics
- Technical issues
  - Surviving network changes
  - Power consumption issues
  - Response time anomalies

Outline

Convincing Organizations

IT services permission

Easy at Dartmouth, due to collaboration with IT services.

Institutional Review Board approval

Research involving human subjects has to be approved by IRB, which operates in terms of medical research.

Convincing the College

DIST had to deal with concerns of the College administration and other on-campus organizations.

- DIST researchers explained the project to the concerned.
- College hired an external auditor to provide feedback.
- DIST added additional layers of security and developed a 20-page document explaining principles & procedures.

Convincing Organizations

IT services permission

Easy at Dartmouth, due to collaboration with IT services.

Institutional Review Board approval

Research involving human subjects has to be approved by IRB, which operates in terms of medical research.

Convincing the College

DIST had to deal with concerns of the College administration and other on-campus organizations.

- DIST researchers explained the project to the concerned.
- College hired an external auditor to provide feedback.
- DIST added additional layers of security and developed a 20-page document explaining principles & procedures.

Convincing Organizations

IT services permission

Easy at Dartmouth, due to collaboration with IT services.

Institutional Review Board approval

Research involving human subjects has to be approved by IRB, which operates in terms of medical research.

Convincing the College

DIST had to deal with concerns of the College administration and other on-campus organizations.

- DIST researchers explained the project to the concerned.
- College hired an external auditor to provide feedback.
- DIST added additional layers of security and developed a 20-page document explaining principles & procedures.

Outline

Privacy Perceptions

As well as convincing the College, the researchers had to convince building owners that DIST would not be a privacy risk.

- Some did not show concern.
- Librarians were sensitized due to new laws and afraid to upset various groups, in part due to their experiences with Patriot Act. In the end, trusted the researchers, relying on public announcements of DIST's activities.
- Student center called, concerned with student reactions and ethics.
- Engineering school asked to come to give a public presentation about security and other technical issues.

Signage

NETWORK EXPERIMENT
in New Hampshire Hall

The Computer Science research project called DIST (Dartmouth Internet Security Testbed) has installed wireless-network monitoring equipment in New Hampshire Hall. The DIST scientists seek to understand the way people use the Dartmouth wireless network and to develop methods for detecting and preventing malicious attempts to disrupt or degrade the wireless network.

The DIST wireless monitors collect routing and signaling information from wireless communications, but discard all content. DIST does not collect e-mail, Web pages, instant messages, or documents; nor does it collect user names, passwords, URLs, or credit card numbers. The routing information that DIST collects is scrambled to obscure the identity of users.

http://www.cs.dartmouth.edu/~dist

Aesthetics

Aesthetics was a much harder problem than researchers expected. DIST deployment for an entire building had to be cancelled for aesthetic reasons.

DIST wireless monitor vs an access point

A Kiewit access point

An open-flap wireless monitor

DIST wireless monitors

An open-flap wireless monitor

A closed-flap wireless monitor

Open-flap and closed-flap monitors, external antennas

Open-flap vs closed-flap

Closed-flap wireless monitors are easier to place than open-flap. But:

- The coverage of internal antennas is only 180 degrees, not 360 degrees.

External antennas vs internal antennas

- External antennas are more powerful than internal. But:
- Internal antennas work better due to antenna diversity.

Open-flap and closed-flap monitors, external antennas

Open-flap vs closed-flap

Closed-flap wireless monitors are easier to place than open-flap. But:

- The coverage of internal antennas is only 180 degrees, not 360 degrees.

External antennas vs internal antennas

- External antennas are more powerful than internal. But:
- Internal antennas work better due to antenna diversity.

Open-flap and closed-flap monitors, external antennas

Open-flap vs closed-flap

Closed-flap wireless monitors are easier to place than open-flap. But:

- The coverage of internal antennas is only 180 degrees, not 360 degrees.

External antennas vs internal antennas

- External antennas are more powerful than internal. But:
- Internal antennas work better due to antenna diversity.

Open-flap and closed-flap monitors, external antennas

Open-flap vs closed-flap

Closed-flap wireless monitors are easier to place than open-flap. But:

- The coverage of internal antennas is only 180 degrees, not 360 degrees.

External antennas vs internal antennas

- External antennas are more powerful than internal. But:
- Internal antennas work better due to antenna diversity.

Open-flap and closed-flap monitors, external antennas

Open-flap vs closed-flap

Closed-flap wireless monitors are easier to place than open-flap. But:

- The coverage of internal antennas is only 180 degrees, not 360 degrees.

External antennas vs internal antennas

- External antennas are more powerful than internal. But:
- Internal antennas work better due to antenna diversity.

DIST monitors that did not make it





DIST monitors that did not make it

The original complaint was aesthetics; the final problem was cost.

DIST monitors that did not make it

Not allowed for aesthetic reasons; placed in the corner to the right instead.

DIST monitors that did not make it

Originally allowed if placed next to the other junk; then denied for aesthetic reasons.

Outline

Pesky Technical Issues

Surviving network changes

Production networks - subnet allocations, VLANs, etc - will change. At least one major change per year is a certainty. Access points must be prepared to survive it.

Power consumption issues

Two ways to power air monitors: Power-over-Ethernet and external power supplies (unsightly). Power stability is essential. AP70s under OpenWRT tend to reboot on power variations.

Response time anomalies

AP70s sometimes take too long to respond to a packet, complicating auditing. Not always clear if it is the fault of AP70s or an artefact of network configuration.

Pesky Technical Issues

Surviving network changes

Production networks - subnet allocations, VLANs, etc - will change. At least one major change per year is a certainty. Access points must be prepared to survive it.

Power consumption issues

Two ways to power air monitors: Power-over-Ethernet and external power supplies (unsightly). Power stability is essential. AP70s under OpenWRT tend to reboot on power variations.

Response time anomalies

AP70s sometimes take too long to respond to a packet, complicating auditing. Not always clear if it is the fault of AP70s or an artefact of network configuration.

Pesky Technical Issues

Surviving network changes

Production networks - subnet allocations, VLANs, etc - will change. At least one major change per year is a certainty. Access points must be prepared to survive it.

Power consumption issues

Two ways to power air monitors: Power-over-Ethernet and external power supplies (unsightly). Power stability is essential. AP70s under OpenWRT tend to reboot on power variations.

Response time anomalies

AP70s sometimes take too long to respond to a packet, complicating auditing. Not always clear if it is the fault of AP70s or an artefact of network configuration.

Thank you!

"There is never enough time.
Thank you for yours!"