Many deployed IoT devices have security vulnerabilities. Vulnerable devices can be used to compromise the whole network. Automatic identification and isolation of vulnerable devices mitigate such threat.

**Challenges in coping with vulnerable devices**

Patching is often impractical:
- Not provided by manufacturer
- Missing facilities for automatic patching
- Technically unsavvy IoT device users

Solution: take a brownfield security approach – identify and isolate vulnerable devices

- Identify device-type (model + SW version) of connected device
- Link device-type to known vulnerabilities (CVE)
- Isolate and filter communications from vulnerable devices

**Device-type identification**

- Fingerprint from device setup communications

\[
F = \begin{array}{cccc}
\text{pkt}_1 & \text{pkt}_2 & \text{pkt}_3 & \ldots & \text{pkt}_n \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
\end{array}
\]

- Random Forest + Edit Distance classification

- Evaluation: Time = 150ms / Accuracy = 82%

**Diagram:**

- IoT Security Service Provider
  - Device Identification
  - Isolation Profile Generation

- Security Gateway
  - Device Fingerprinting
  - Enforcement Rule DB

- Device setup communications

- Untrusted network
  - strict
  - restricted

- Trusted network
  - trusted

- Classification performance for 27 devices