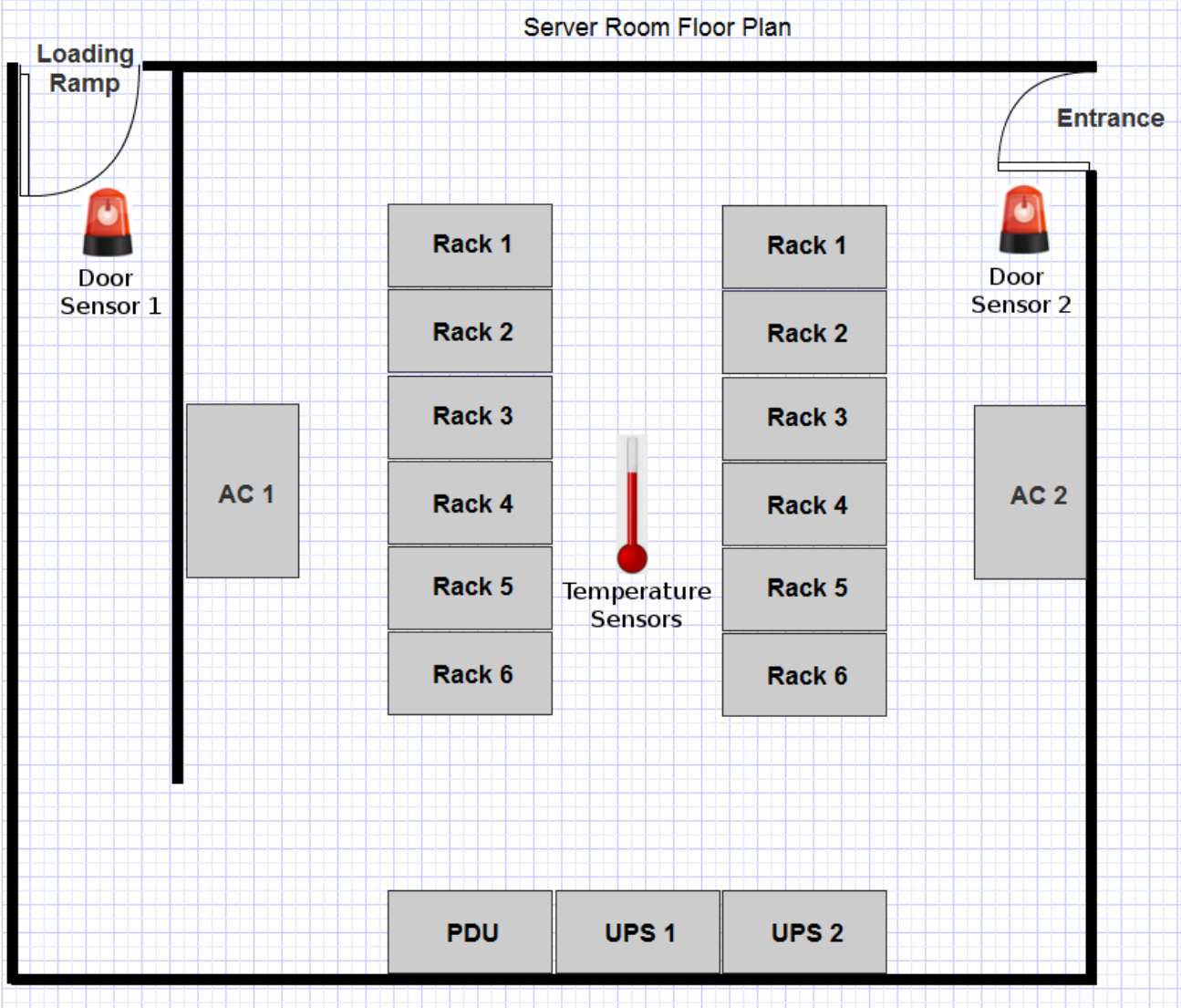
Under New Management: Practical Attacks on SNMPv3

Nigel Lawrence and Patrick Traynor

Where is SNMP used?

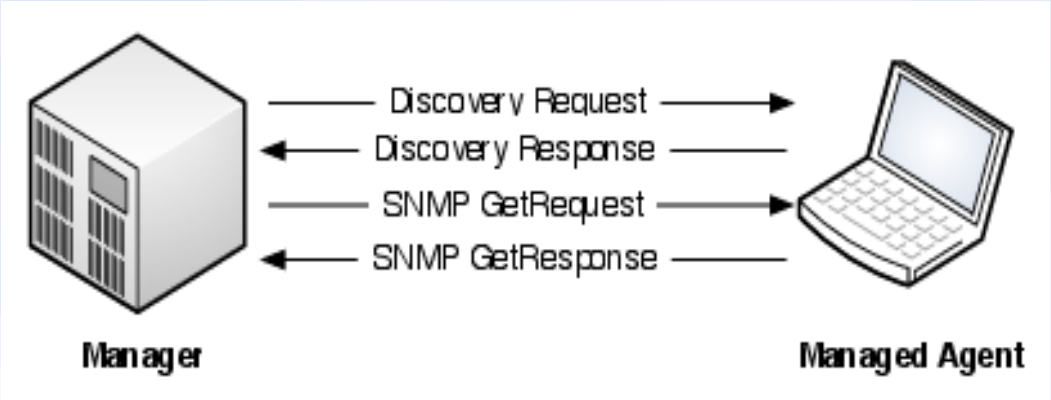


Introduction

- Motivation
  - Ubiquity and importance of SNMP
  - Little previous analysis
- Goal
  - Examine weaknesses in SNMPv3
  - Exploit the protocol
  - Determine mitigation strategies

Overview of SNMPv3

- Purpose and goals
- SNMP get and set requests
- Authentication and encryption
- Key localization
- Discovery process



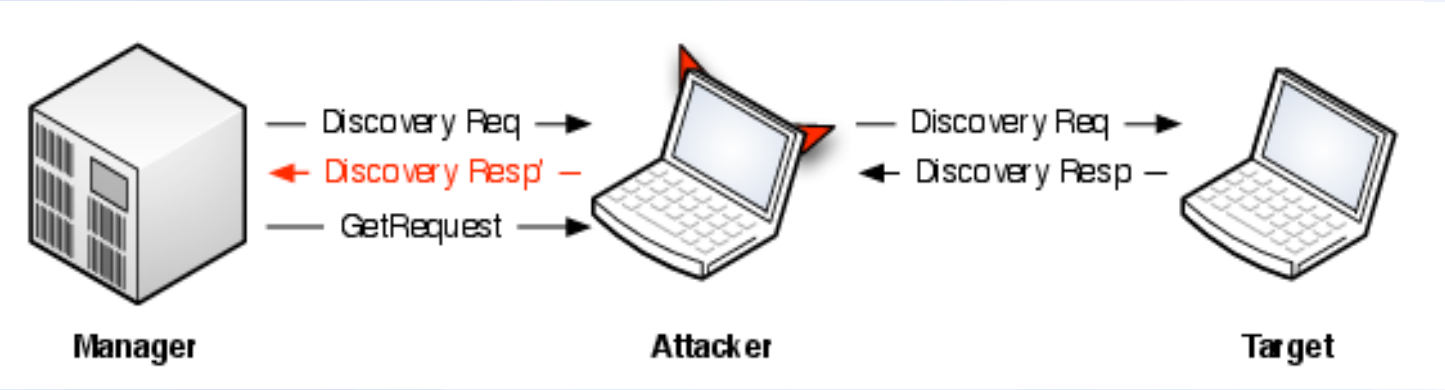
Vulnerabilities

- Reliance on Discovery
  - snmpEngineIds *should not* be exchanged in cleartext.
- Lack of Authentication
  - Managers have no way to distinguish between agents

Reading Requests

- Requirements
  - Man-in-the-middle (MITM)
  - Compromised key
- Modify the snmpEngineId
- Decrypt the packet

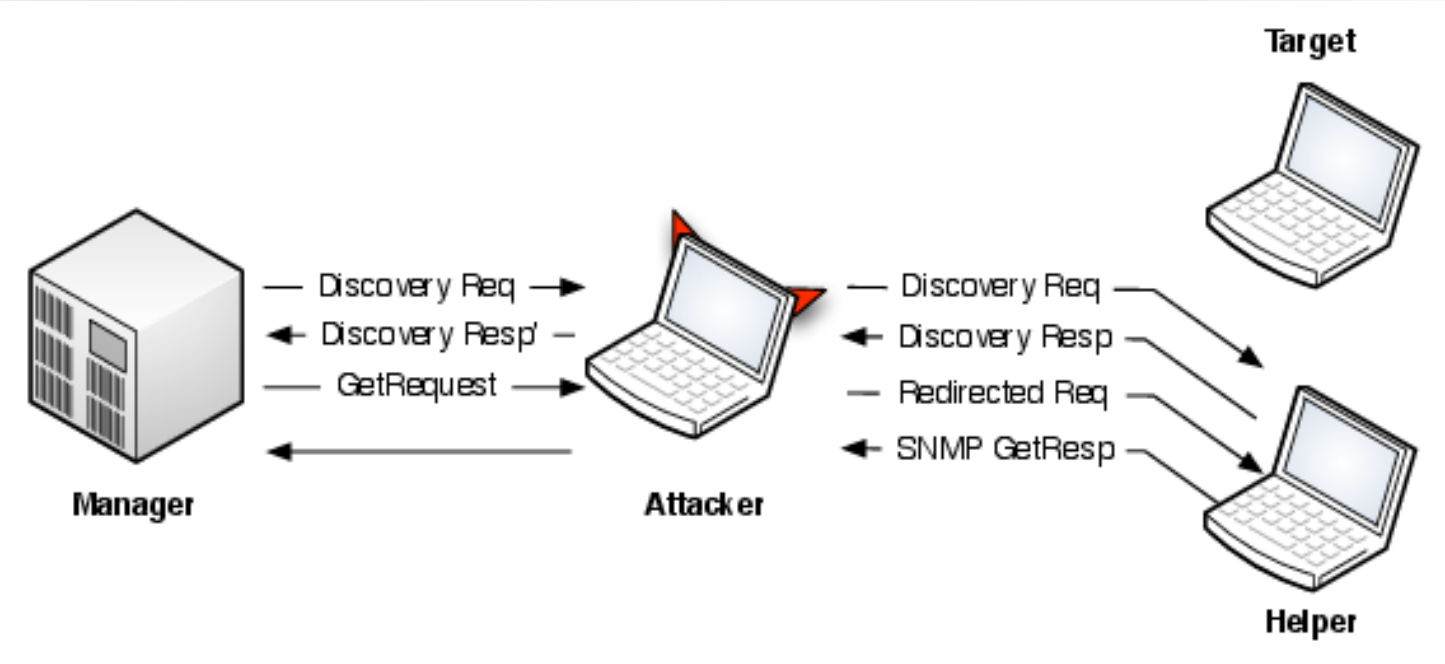
Reading Requests



Redirecting Requests

- Requirements
  - MITM and “helper” agent using DHCP
- Modify discovery messages
- DHCP spoofing
  - Control helper's IP address
- Caching
  - Ensure delivery of packets
- Gratuitous ARP

Redirecting Requests



Implications for the Protocol

- Key localization is ineffective
- Agent responses are indistinguishable
- Responses can be spoofed with a compromised key
- SNMP set requests are also vulnerable

Nagios before spoofing

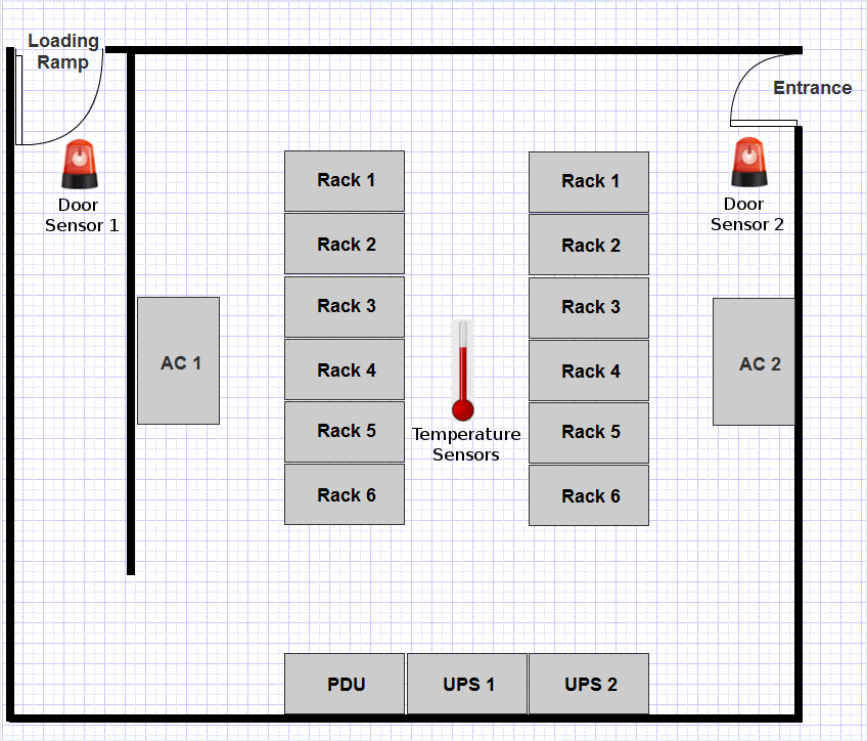
Host	Service	Status	Last Check	Duration	Attempt	Status Information
helper	Hostname	OK	04-28-2012 18:15:33	13d 3h 29m 40s	1/1	SNMP OK - helper
target	Hostname	OK	04-28-2012 18:15:34	0d 0h 10m 49s	1/1	SNMP OK - target

Nagios after spoofing

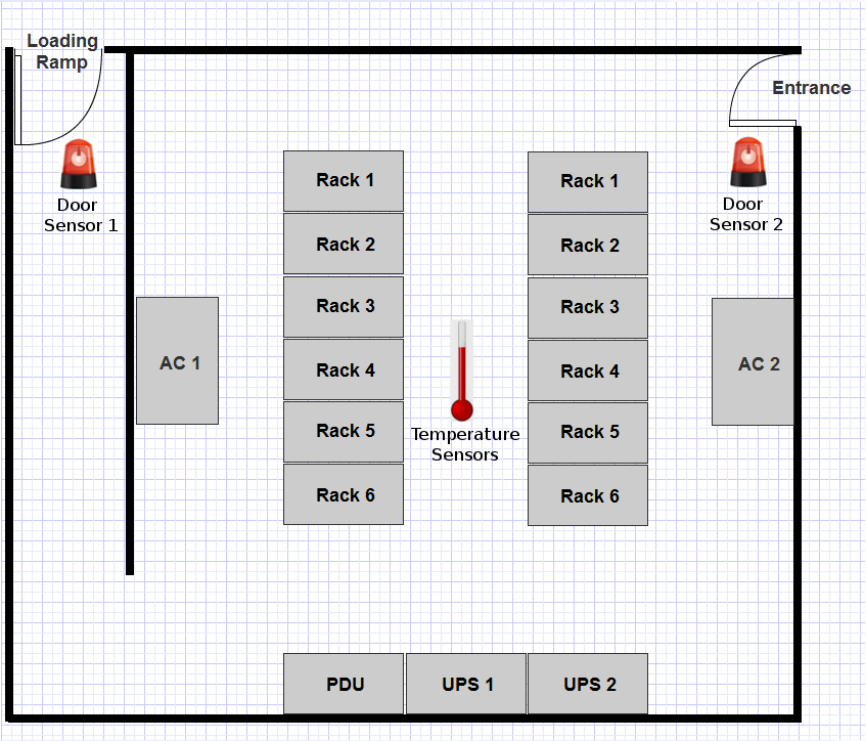
Host	Service	Status	Last Check	Duration	Attempt	Status Information
helper	Hostname	OK	04-28-2012 18:19:33	13d 3h 33m 51s	1/1	SNMP OK - helper
target	Hostname	OK	04-28-2012 18:19:34	0d 0h 15m 0s	1/1	SNMP OK - helper

Example Attack

Server Room A



Server Room B



Mitigation Strategies

- Protect the transport layer
  - IPsec or TSM
  - Sometimes this is impractical
- Modify the protocol
  - Don't trust discovery for snmpEngineId
  - Still useful for clock synchronization
- No changes to individual agents

Questions?