



# M2M Security

## An Evolving Landscape

**Chris Foley**

Principal



9-November-2011

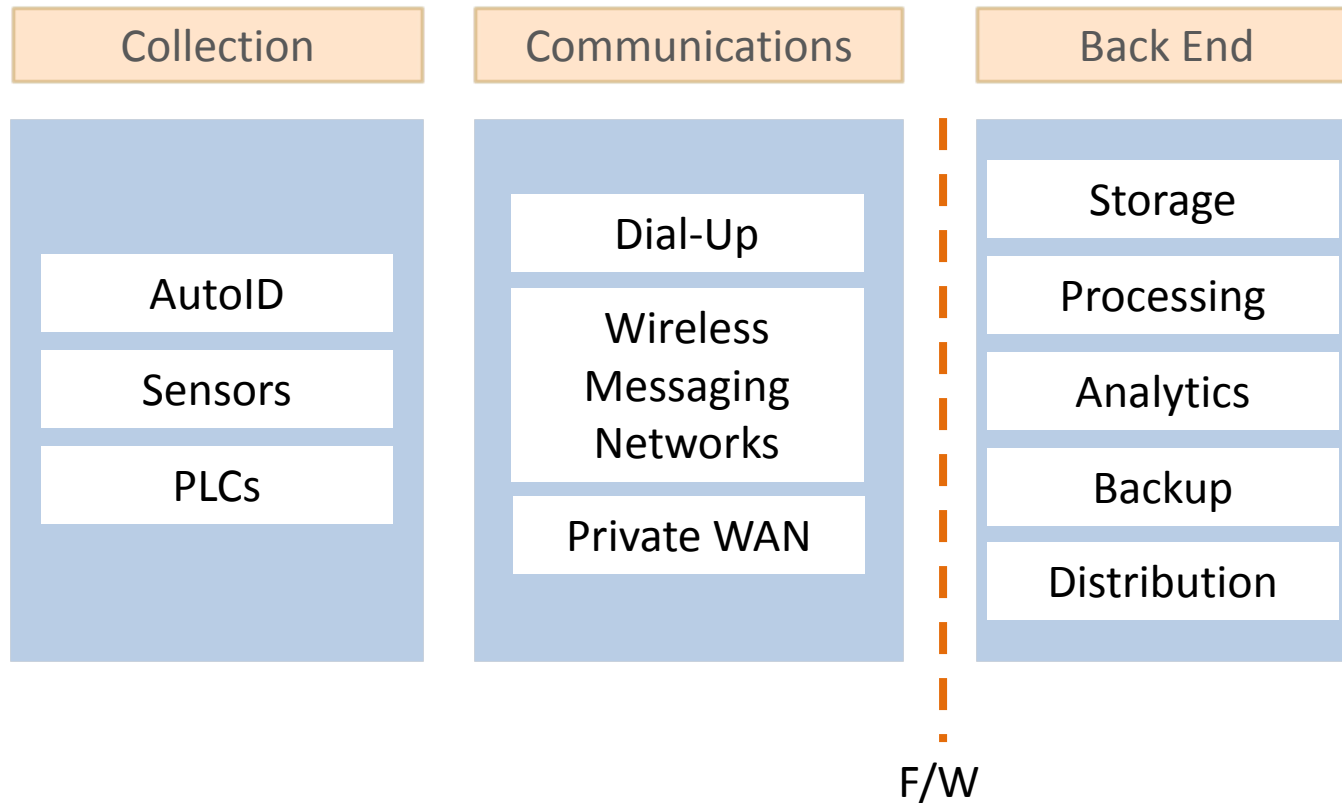
# The Traditional M2M Definition

## M2M: Machine-to-Machine

The collection storage, monitoring, and transmittal of data between two or more unattended devices (machines)

- Classic M2M examples are Automated Meter Reading (AMR) and remote asset or premises monitoring (telematics on vehicles, flow meters, intrusion detection, etc...)

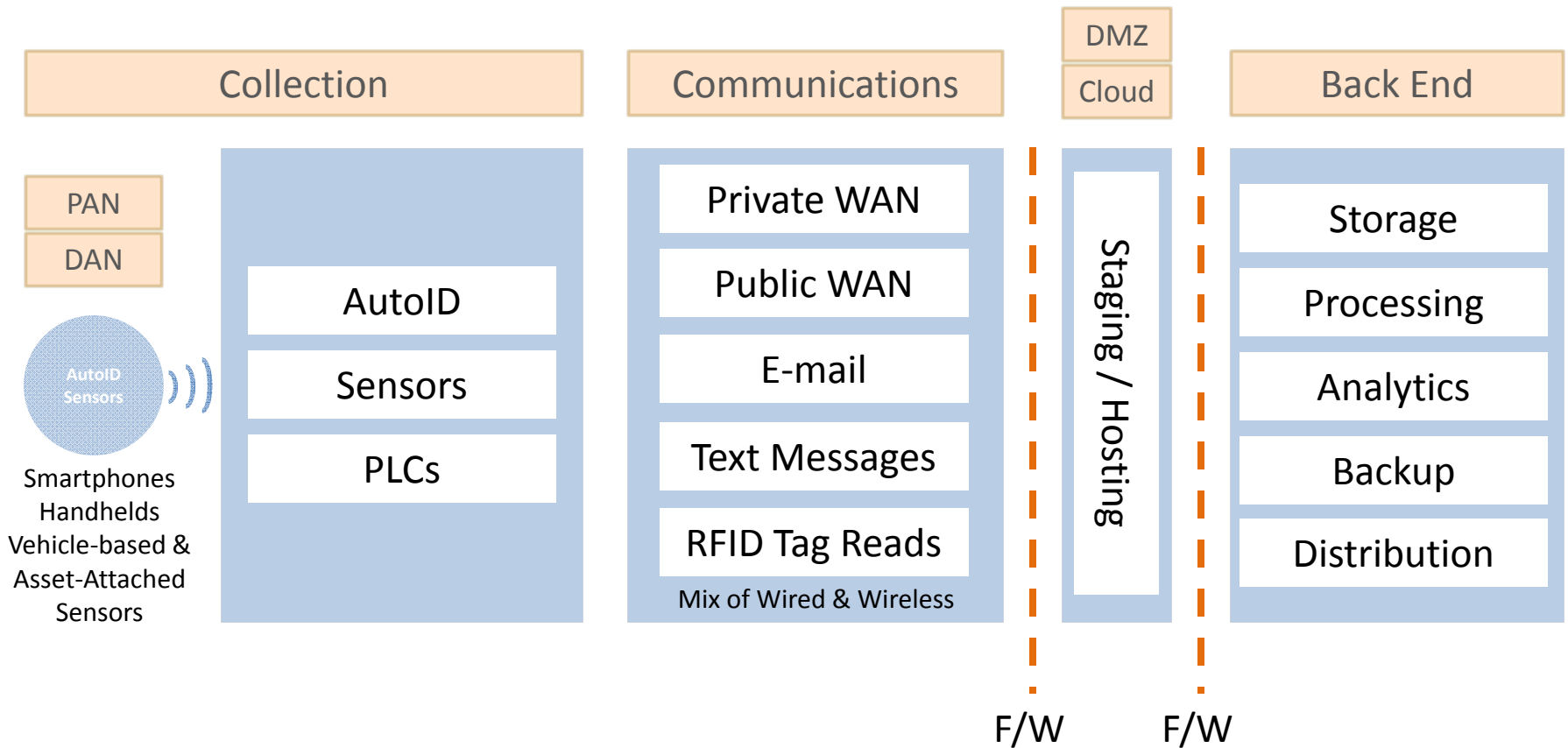
# Traditional M2M Security Zones



# RFID & Mobiles Extend the Model

- RFID tags are free-floating M2M components
  - ❑ Not associated with any one device or location
  - ❑ Often not physically secured
  - ❑ Perform data collection, data storage and data communication roles
- Mobile Phones
  - ❑ Intermittently-attended devices
  - ❑ Ad hoc peer-to-peer connections
  - ❑ Subject to loss or theft
  - ❑ Can acquire, store and transmit M2M data
  - ❑ NFC-enabled phones can perform both data collection and data origination roles (Hot-spot tag reads, e-wallet authorizations)

# Today's M2M Security Zones



# End-to-End or Risk-based Security?

- Access and/or Control of each segment?
  - Network and data hosting SLAs available?
- Value of M2M data to third parties
  - Time and effort required expose data
- Is context or attribution of data also exposed?
- Legal or regulatory requirements?
  - Responsible for which segments?
- Relative exposure of each segment

# Security at Point of Collection

- What Needs Protection?
  - Remote and Mobile Devices (outside the firewall)
    - Staged Data on device or removable media
    - Streaming Data over multiple wireless bearers
    - Application Interfaces
  - Fixed-site Infrastructure (inside the firewall)
    - PLCs
    - Servers, Network-Attached Storage
    - Wireless Access Points, Switches & Routers
    - Application Interfaces
- Protection Options
  - Traditional IT security in physically-secured environments
  - Device lockdown or data expiry on mobile or partially-attended devices
  - FIPS-level hardware and/or software data protection on unattended or remote devices
  - Device-based or remotely-accessible applications removed or locked-down
  - Prohibit or cripple removable storage access on M2M devices

# Security of Data in Transit

## Common M2M Communications Protocols and Standards

- IP-enabled devices frequently required to support RSA 1024- and 2048-bit private key encryption, 3DES, AES-128/192/256, ARC4, MD5 and SHA-1
- SSL v.3/Transport Layer Socket v.1 (SSL3/TLS1) for socket-based traffic
- FTPS (Secure FTP) for file transfers
- SMTPS (Secure SMTP) S/MIME, POP3S for message-based communications
- Bluetooth & other short-range internode communication protocols (some proprietary)
- AS2 required in many multi-party or supply chain-related EDI communications

## Implementation Options

- Security modules embedded in IP-enabled M2M hubs or nodes
- Third-party “black box” hardware security communication appliances
- Software-based encryption within the application (slower, but cheaper)
- Proprietary segmentation, data masking or use of non-attributable data

# Security of Staged & Hosted Data

- Required in store-and-forward and cloud architectures
- Data integrity, data vulnerability, or both?
  - Data Integrity
    - Restart / power-loss survivability
    - Flash-based or other nonvolatile storage
    - Locking of rewritable tag-based data
  - Data Vulnerability
    - FIPS-class hardware and/or software encryption
    - HIPPA considerations – data masking
    - Protection from interrogation by rogue systems
    - Encryption of tag-based data

# Back-End Security

- DMZs may be necessary in multi-party or shared-access M2M scenarios
- Multitenancy required in cloud-based models
- Once behind the firewall, M2M data under the traditional IT security umbrella
  - Insulated by firewalls and subnet architectures
  - Encrypted as-required on internal storage systems
  - Network access control kicks in
  - Scheduled backups ensure data retention

# Summary

- M2M is increasingly pervasive
  - We all now carry M2M-capable devices
- Amorphous roles of new devices create both M2M opportunities and points of exposure points
- Traditional IT security model only applies at back-end
- Reliance on third-party SLAs frequently required for end-to-end security
- Cloud model also introduces new exposure points
- Risk-based security model should be weighed before attempting to implement end-to-end M2M schemes