OneM2M Security Requirements

Mihai Voicu, PhD
CSO

ILS Technology LLC

Security – why now?

Value

- Should support and enhance in value of any architecture
- Creates competitive edge
- Create business value
- Becomes very costly if it is not properly implemented

Importance

- The same importance with architecture, therefore must be included in the discussions from the beginning
- Must be backed in the architecture and requirements
- How many times the word security came in any discussions

Risk

- Minimize the exposure
- Security is no longer a plug-in
- Examples are everywhere: Microsoft (IE, Windows XP - 7), Apple (MobileMe, but not the MAC OSX)

We're moving toward a world of

... cloud-based ***continuous services*** that connect us all

… appliance-like ***connected devices*** enabling us to interact with those cloud-based services

Ray Ozzie (Chief Software Architect at Microsoft)
"Dawn of a New Day" - Farewell Letter

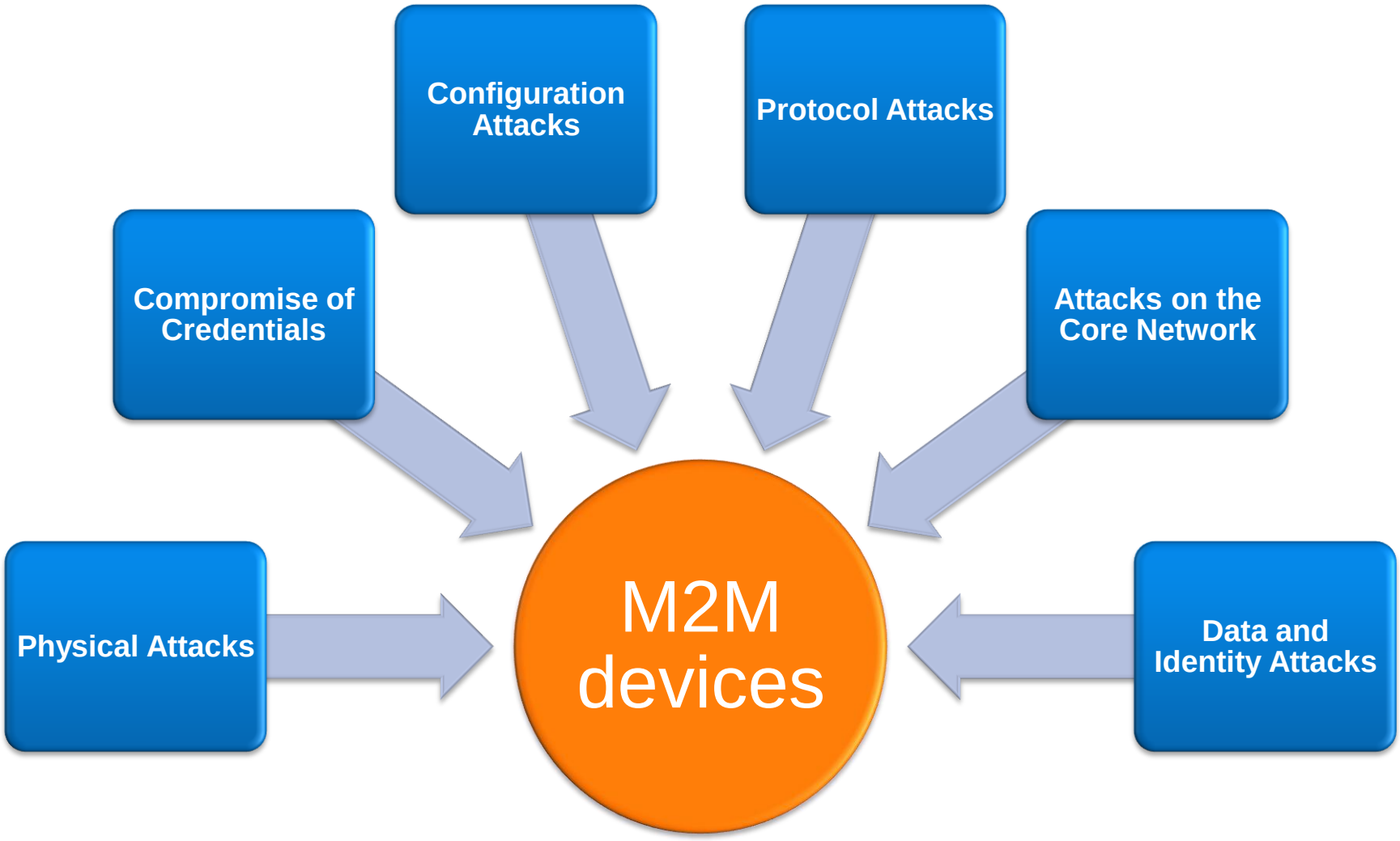
Space Definition

M2M involves communication without (or only limited) human intervention.

M2M is about technologies that allow connections between remote devices and systems

M2M communication can use both wireless and wired networks.

Security Vulnerabilities



Security Fundamentals

Confidentiality

- Prevent the disclosure of information to unauthorized individuals or systems

Integrity

- Data cannot be modified undetectably

Authenticity

- Data is genuine

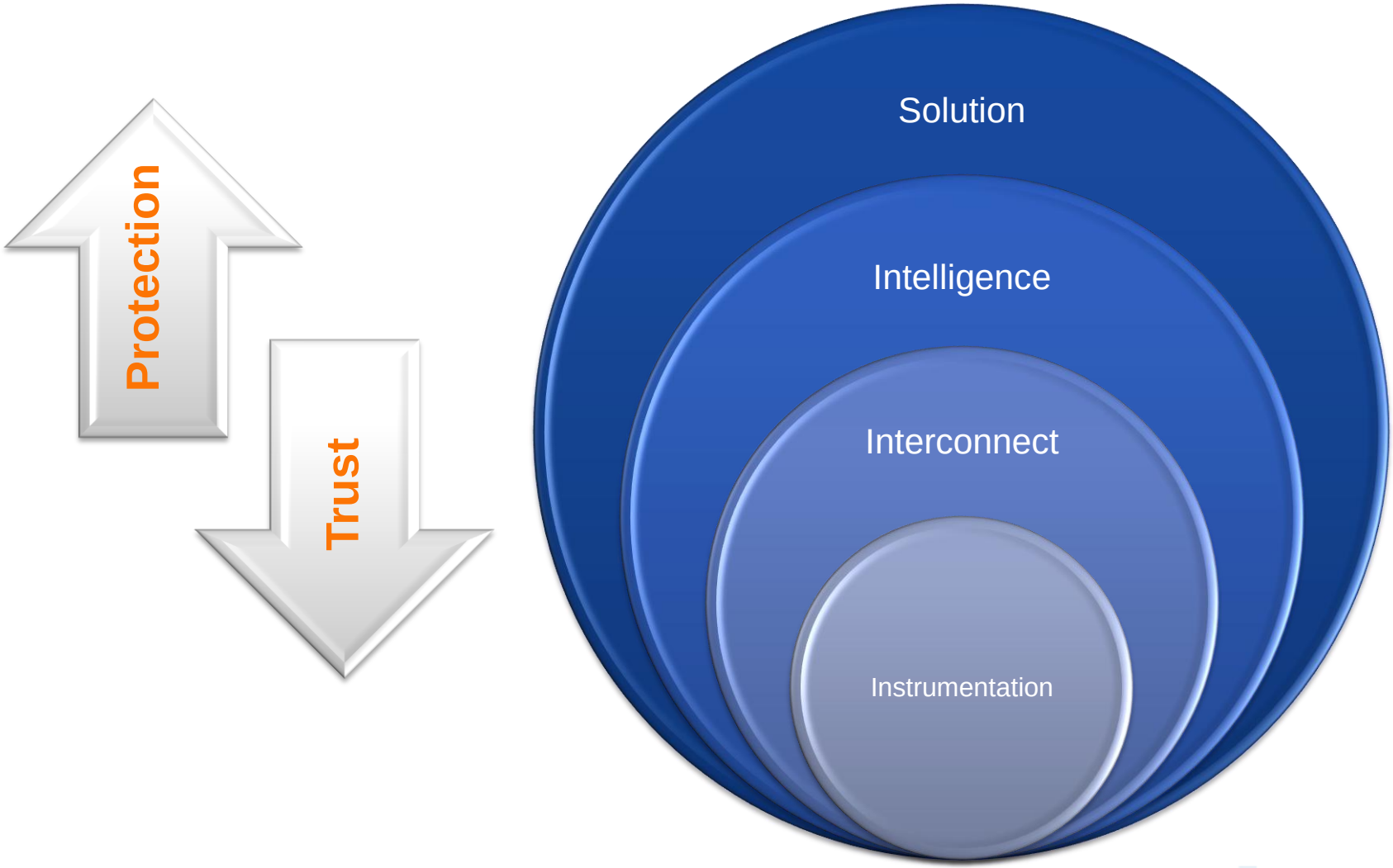
NIST Recommendations

Security for the Smart Grid networks

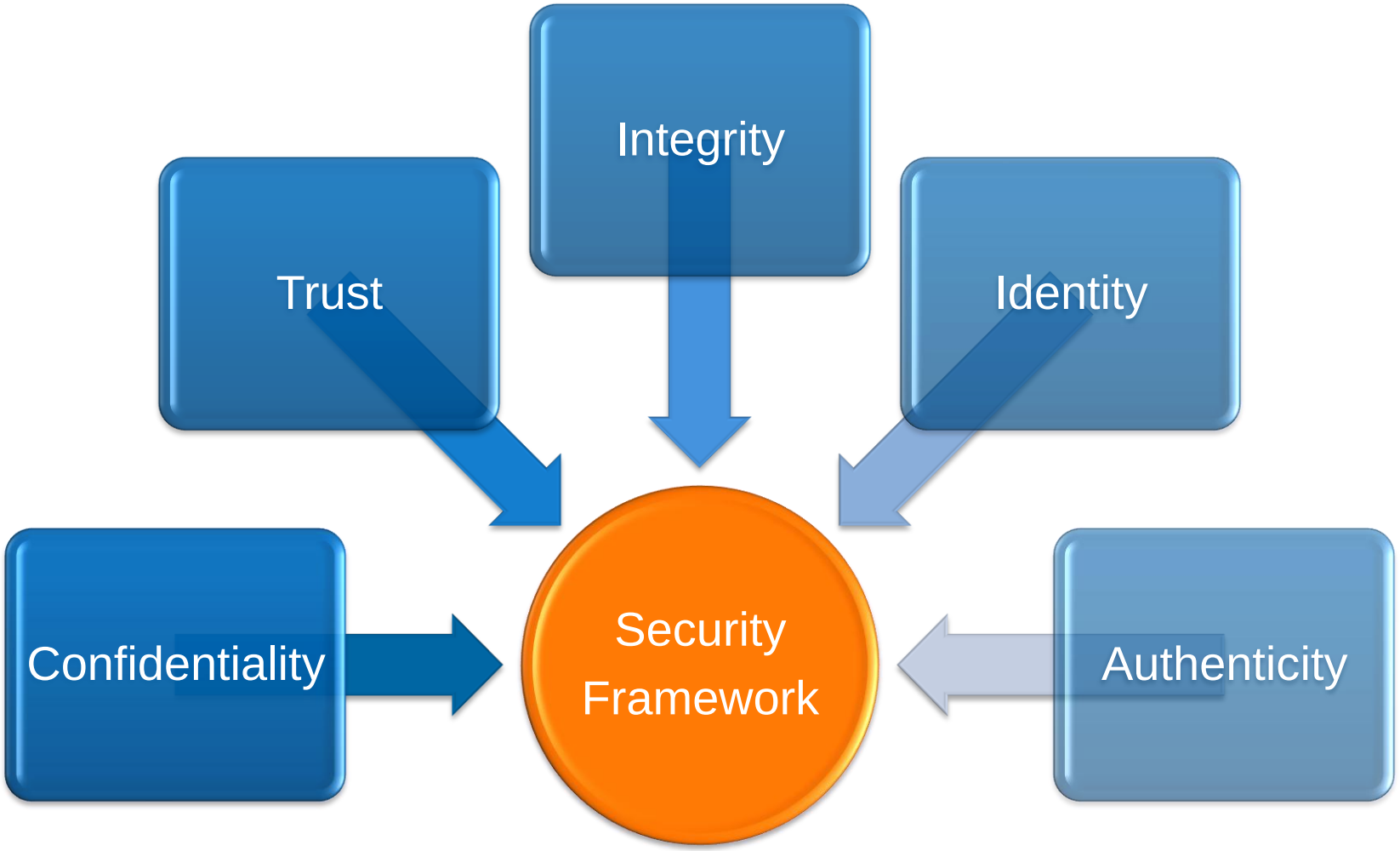
- Security policies, procedures, and protocols to protect information and commands in transit or residing in devices and systems
- Authentication policies, procedures, protocols
- Security policies, procedures, protocols, and controls to protect infrastructure components and the interconnected networks

Smart Devices Security Architecture

Defense-in-depth Security



Security Framework



Required Security Features

Authorization and Authentication

RBAC - Role-based Access Control

Data Validation

Session Management

Data Integrity and Confidentiality

Auditing and Monitoring

Trusted Environment

Authorization and Authentication

- Employ the best in class for authentication of the smart devices:
  - LDAP, Active Directory
- Each device must be identifiable
- Every smart device must be able to authenticate with a central or distributed authorization engine before accessing the system
- Every device must be able to be authorized to perform specific tasks.

RBAC - Role-based access control

- Basics
  - "Device" role must be authorized – role authorization
  - Operations can be executed only if the "device" has the proper role – role assignment
- Very difficult to implement for non-smart devices
- Permissions calculated based on roles and groups
- Inheritance plays a fundamental role
- Use of the Least Privilege principle

Data Validation

- Data between devices must be checked for validity before processing.
- If clients and/or server are available, input/output data type and range must be validated.
- If databases available, data type and range must be validated.
- Correct data validation rules must be available to avoid:
  - Data corruption
  - Security Vulnerabilities
  - Etc..

Session Management

- Transactions across security zones must use the correct transaction mechanism to reduce the thread of session hi-jacking
- Implement the necessary security context that includes authentication and authorization steps
- Making sure that volatile session data is properly deleted
- Logging on session information is not reveling confidential information

Data Integrity and Confidentiality

- Making sure that the data gets across security zones without being altered
- Data stored or in transit should be able to use encryption
- Making sure that the data is received from an identifiable source.

Auditing and Monitoring

- Smart devices must be able to record information about:
  - Devices access
  - Users Access
  - Configuration Changes
  - Session details
  - Etc..
- Must be able to produce simple or complex reports

Trusted Environment

- For hardware manufactures
  - Trusted platforms
  - Integrated chips to validate the device identity
- For software manufactures
  - SDLC guidelines
  - Core processing code-signing
  - Plug-ins code-signing
  - Code maintenance
- Specific security procedures for:
  - Vulnerability monitoring
  - Incident response
  - Disaster Recovery.
- Security Standards – ISO 27001, CoBIT, ITIL…

Thank You

Mihai Voicu, PhD
Chief Security Officer

ILS Technology LLC
mvoicu@ilstechnology.com