IBM Research

Machine-to-Machine Security and Privacy: Challenges and Opportunities

David W. Kravitz
Information Security Group
IBM Almaden Research Center

No out-of-band- acquired context off of which to bootstrap “identity-based” communications

- Disadvantage: Not as simple as knowing each other’s mobile phone numbers, email addresses, and maybe shared “secrets” (e.g., children’s birthdates or what restaurant or occasion they last dined at together)
  - Pure M2M lacks such information for use to set up or test who is at the other end of a communication
  - Service providers communicating with devices as endpoints cannot rely on this type of data to attempt to detect “impersonation” or cloning of authorized accounts
- Advantage: By not basing security and privacy on data points that are increasingly easy to seek out via social networks and Internet search, perhaps M2M security can have a stronger underpinning
  - Not only is data required for successful identity-fraud more available than ever: also new ability to anonymously acquire convincing counterfeit physical credentials/IDs anonymously (e.g., via Bitcoin)

M2M and H2M do not operate under the same set of requirements/constraints

- H2M: user capability to contact a service provider via arbitrary/multiple client devices, which may be multi-user, operated or managed by others, untrusted to store credentials
  - Can supplement passwords and security questions with other factors of authentication
    - But one or more such factors may be unavailable
      - > lost or forgotten phone
      - > transaction to a merchant that is not on existing white-list stored at counter-signing authority (e.g., Bitcoin multi-signature transaction)
- M2M: sensors may be unmanned/buried, have non-rechargeable batteries, be highly constrained (e.g., memory and computation)
  - Unanticipated/malicious battery drainage, device tamper…
    - may have to be remotely detectable

Continuity assuredness (i.e., same device as communicated with before without fear of impersonation)

- E.g., Telehash: https://github.com/telehash/telehash.org/blob/master/protocol.md
  - "because each application instance or device generates its own public/private keypair, they cannot be impersonated and security is not dependent on trust in certificate authorities"
- While important, this continuity is not the same as actually knowing who/what the node corresponds to

Replay-/compromise-/cloning- detection

- M2M systems may require new or different mechanisms and analytics techniques for anomaly detection
  - No “users” to call ahead to apprise system of plans
  - No human factors, such as sleep times/meal times

Trust via consensus (decentralization) vs. trust via contractual obligation (Certification Authorities and Registration Authorities)

- Public Key Infrastructure (e.g., public key certificates) vs. Privilege Management Infrastructure (e.g., attribute certificates)
  - How complete/unchangeable is knowledge about devices at time of initial provisioning?
  - Roles/attributes may change more frequently than key pairs
  - Leveraging hardware roots of trust and cross-certification

The human element behind the scenes of M2M

- Incentives (e.g., financial compensation for first successful relevant proof-of-work)
- Disincentives/don’t cares (e.g., the good of the system vs. the good of the individual)
  - Using limited resources of node A for distribution of a high-priority firmware upgrade of node B at the expense of the current user of node A

Matching connectivity and communications topologies to use cases (may be a mix)

- One-way or bidirectional communications; one-way or bidirectional authentication
- “cloud” involved to offload computation/storage or for analytics
- Home hubs/gateways; remote hubs/gateways
- P2P
- 1-1; 1-many; many-1
- Pre-established cross-platform provisioning of keying material vs. ad hoc participating entities
  - Symmetric keys vs. asymmetric key pairs
- Dynamically managing joining and leaving of nodes
- Revocation and renewability
- Latency and redundancy considerations

Matching identity management to use cases

- Low-to-moderate- value transactions conducted anonymously/pseudonymously may benefit from low overhead
- High-value transactions may require accountability/reversibility through verifiable identities
- Healthcare: medical devices communicating with hospital
  - Good audit trails not enough: requires up-front confirmation of attributes/authorizations/permitted functionality of nodes

Whose data is it? What comprises legitimate vs. illegitimate uses of the data?

- Data ownership, management, and distribution (in raw or sanitized/aggregated form)
- Smart grid/smart home/smart office: deep knowledge of usage patterns and anomalies as byproduct of core system usage
  - Of interest to advertisers
  - Of interest for timing home-break-ins
  - Of interest to competitors (industrial espionage)
- Medical devices, smart pill bottle tracking, smart fridge consumption tracking: benefits (promotes better health) and liabilities (higher insurance premiums for non-compliance?)