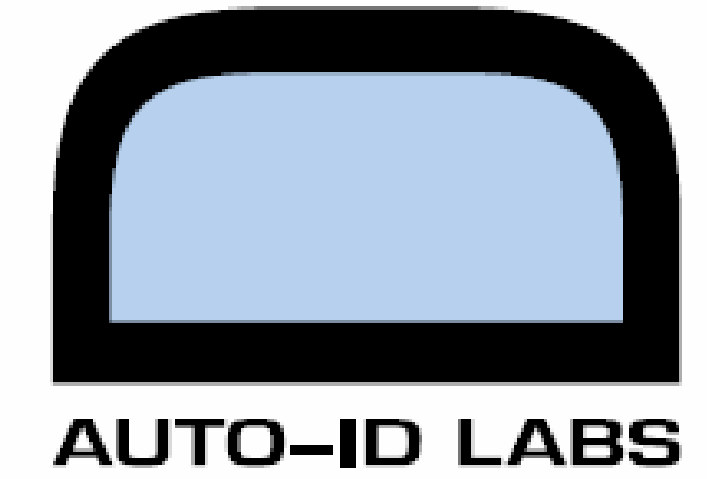


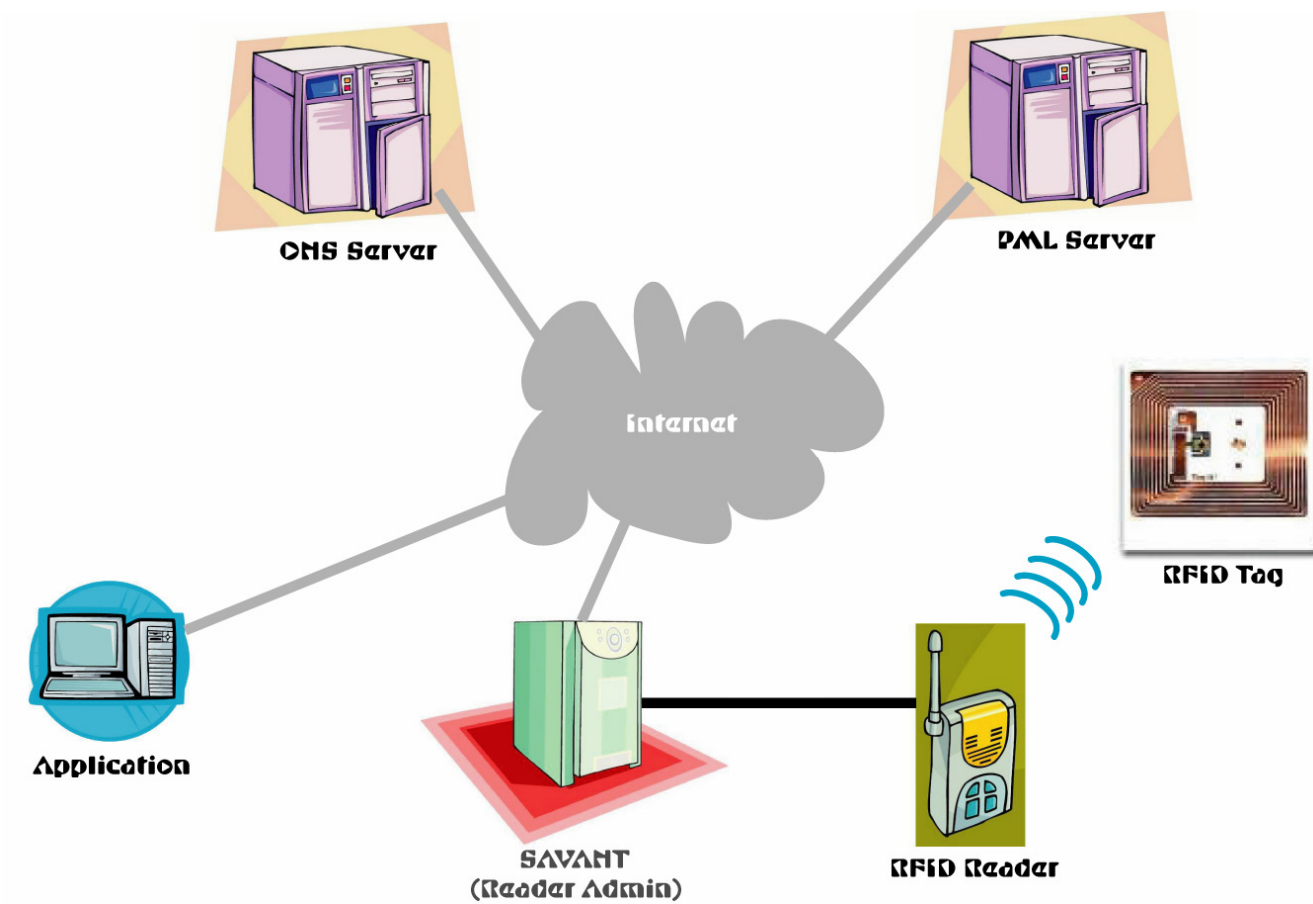


RFID End-to-End Security

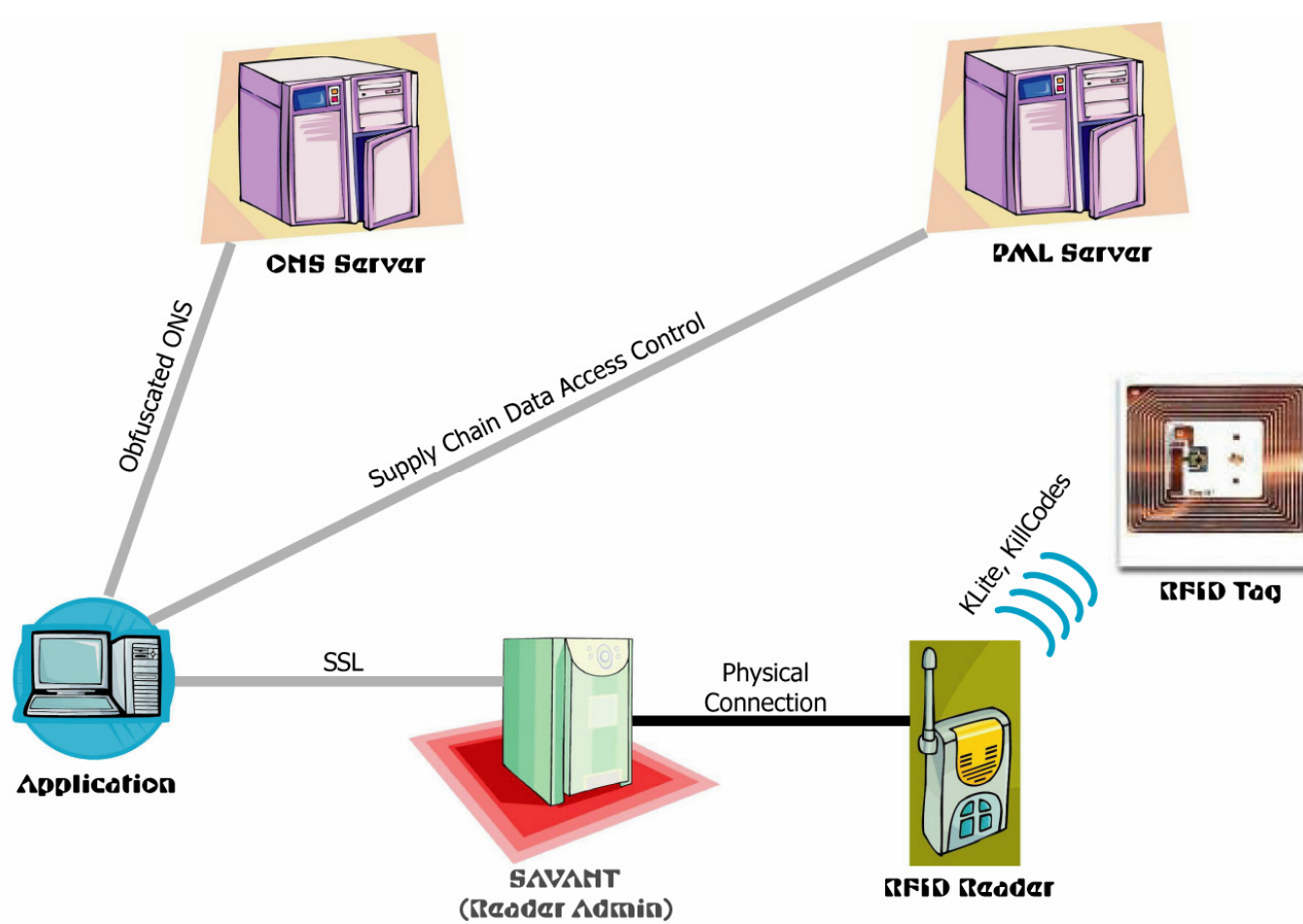


Motivation

Radio Frequency Identification (RFID) is becoming a critical component in a variety of systems, including passports, retail inventory and theft prevention, and medical tracking. However, all of these systems lack protection at a variety of levels. This project addresses the weaknesses in current RFID applications and provides a new abstraction that protects the application.



Physical Connections in a Standard RFID Application



Logistical Connections in a Standard RFID Application

By Joe Foley

MIT Auto-ID Laboratory

KLite

KLite is a simple hash-based authentication mechanism used to prove the legitimacy of a tag. This is to prevent unauthorized copying, in addition.

Attacks

- Passive Listening
- Traffic Analysis
- Malicious Hardware
- Corrupt Administrators
- RF and Ethernet
- Forgery

Operation

1. R gets ID from T
2. R makes random C, sends to T
3. T generates $H_1(S,C)$, sends to R
4. R sends (ID,C) to V
5. V looks up S for V, generates $H_2(S,C)$ and sends to R
6. R compares $H_1(S,C)$, $H_2(S,C)$ to verify

Limitations

- Tag State
- Tag Cryptographic Hash Capability¹
- ID Sent in Clear

Adaptive Obfuscation

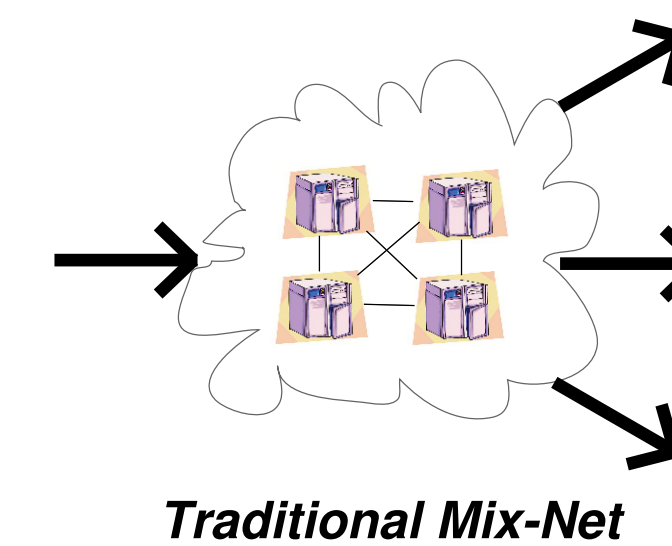
Obfuscation attempts to hide legitimate data by also having fake data that it can disappear into. Adaptive Obfuscation takes this one step further by composing data that looks real, but is not useful.

Needs:

- Pseudo-Legitimate Chaff
- Repeat Queries
- Adaptive Routing
- Protection of Anti-Collision Discovery
- Flypaper – “juicy” fake data

Methods

- Mix-Nets
- Mapping one Tag ID space to another
- Temporary False Identity
- Sustained False Identities



Generic Access Control

Generic Access Control driven by the need for a ubiquitous and intuitive method for any application to control data visibility and updates.

Needs:

- Arbitrary-Grained Access Control
- Extensible and Distributed
- Positive and Negative Set ACL construction
- Real-time Updates
- Adaptive to network segmentation - failsafe

Methods

- SIREN: Role Based Access Control²
- XML-based Role Based Access Control
- HL7
- Government Information Control Methods

1. Stephen August Weis. Security and Privacy in Radio-Frequency Identification devices. Master's Thesis, MIT.
 2. Arundhati Sing. SIREN: A SQL-Based Implementation of Role-Based Access Control for Enterprise Networks. Master's Thesis, MIT.

Applications

National Security

The introduction of RFID tags into passports has made it even more necessary that anti-counterfeit technology be developed. Any RFID system that is used for a method of identification needs to guarantee that the ID cannot be trivially forged or copied.



Brand and Liability Protection



Drug manufacturers need a way to prove liability for pharmaceuticals when there is a problem or simply to track a drug trial. Proof that an item is genuine and not a forgery is critical

Asset and Information Protection

Retailers, and those who have more special needs such as government and medical regulations on privacy make it necessary to ensure that an asset has not been swapped for an empty. For example: weapons, supplies, etc.

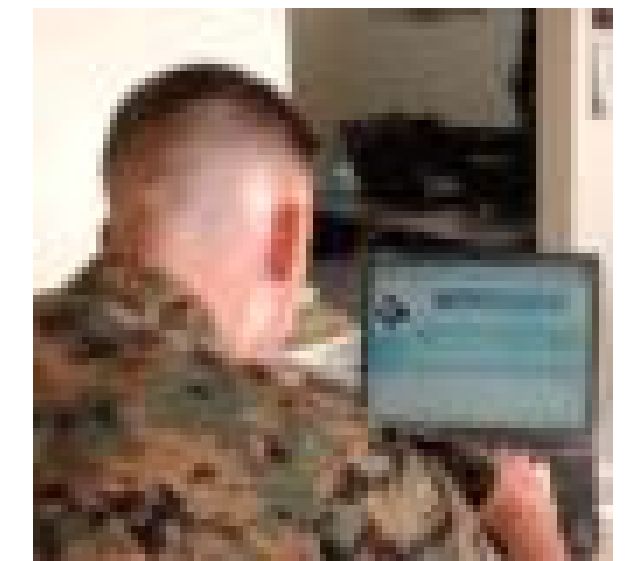


Image Sources: (Top to Bottom)
http://www.bbc.co.uk/1/auyaues/spanish/1/moving_on/challenge/passport.shtml
<http://jamesburnsdesign.com/images/3DExamples/PillBottle.jpg>
http://admin.avisian.com/images/rfid_marines.gif