Breaking the back end!

DefCon 27, Las Vegas 2019
Overview

+ Transit System
+ Reverse Engineering
+ My Discoveries
+ The Exploit
+ The Lessons
How This Is Different

- This is not illegal
  - We aren’t sneaking into the station
  - We aren’t hacking their terminals
  - We aren’t social engineering anyone or attacking their wired/wireless network
- This is not about the hardware
  - We aren’t cracking anyone’s encryption
  - We aren’t cloning the magstripe, RFID, or NFC
How This Is Different

This Is About

- Flaws in the Application Logic
- OK. Cloning is involved but it is not the vulnerability exploited
- Using AppSec to attack Complex Multi-Layered Real World Solutions
Elevated Train

- **Bangkok Mass Transit System (BTS)**
- Elevated rapid transit system in Bangkok, Thailand
- Serves Greater Bangkok Area
- Operated by Bangkok Mass Transit System PCL (BTSC)
- 43 stations along two lines
Tickets

- Stored-Value Card (NFC)
- All Day Pass (Magstripe) and Single Journey (Magstripe)
Tickets

- Two magstripes
- Hole through one magstripe
- Only 0.27mm thick
Tickets
Tickets
The Equipment

- Standard Reader/Writer
- Manufactured in China
- Standards or Raw Read
- Errors Rare
- Reliable Performance
Lab Work

- Attempted Decode Using Standards
  - International Organization for Standardization
  - 6-bit Character sets and 4-bit Character sets
  - Some With Parity and Some Without
- Attempted Decode both forwards and backwards
- It wasn’t using the standards
Lab Work

- There is no encryption.
- There are no parity checks.
- There was no longitudinal redundancy check (LRC).
- There are no timestamps.
Field Work

- The section “7826” is the Ticket Type
- The section “00FF74” is always 100 + the price of the ticket
- For all day passes, the section “00FF74” is used to track trips taken
# Field Work

<table>
<thead>
<tr>
<th>Date</th>
<th>Batch</th>
<th>Station</th>
<th>GUID First</th>
<th>GUID Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>15</td>
<td>Ari</td>
<td>D0403AE7 F51CC51D</td>
<td>00D60F F5A889A6C5</td>
</tr>
<tr>
<td>2017</td>
<td>22</td>
<td>Ari</td>
<td>E0406C15 F52CD5A9</td>
<td>00D60F F5A88AA67B</td>
</tr>
<tr>
<td>10/25/2017</td>
<td>15</td>
<td>Ari</td>
<td>A341760E B02D364D</td>
<td>00D20F B081A6087B</td>
</tr>
<tr>
<td>10/25/2017</td>
<td>15</td>
<td>Ari</td>
<td>7A4101A9 B02D46D4</td>
<td>00D60F B081A72AC5</td>
</tr>
<tr>
<td>9/1/2018</td>
<td>15</td>
<td>Ari</td>
<td>78401A32 E9175ED</td>
<td>00D20F E948A00A41</td>
</tr>
<tr>
<td>9/15/2018</td>
<td>15</td>
<td>Sanam Pao</td>
<td>E542D0E4 FB1EA6FC</td>
<td>00C20E FBD88D38D2</td>
</tr>
<tr>
<td>9/20/2018</td>
<td>15</td>
<td>Sanam Pao</td>
<td>E64211A5 FC2E843A</td>
<td>00C20E FCE093343B</td>
</tr>
<tr>
<td>9/30/2018</td>
<td>15</td>
<td>Ari</td>
<td>32404A91 062FF509</td>
<td>00D60F 0631D72460</td>
</tr>
<tr>
<td>9/30/2018</td>
<td>23</td>
<td>Ari</td>
<td>FF421102 061F35FF</td>
<td>00D60F 0631D72498</td>
</tr>
<tr>
<td>10/7/2018</td>
<td>15</td>
<td>Ari</td>
<td>03430838 0D2F7759</td>
<td>00D20F 0D697408E8</td>
</tr>
<tr>
<td>10/15/2018</td>
<td>140</td>
<td>Sanam Pao</td>
<td>E9D619E36 192FE79A</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>11/1/2018</td>
<td>140</td>
<td>Sanam Pao</td>
<td>E9D64094 262FF7C9</td>
<td>00E20F 26317E1CC0</td>
</tr>
</tbody>
</table>
Field Work

Buying

0x00E078401A327826E91E76ED00FF7400D2D0E948AE04A1

“Issued”

Entering

0x00E078401A327826E91E76ED00FF74801C0FE948D8681B

“Used”

Exiting

0x00E078401A327826E91E76ED00FF74801C0FE948D8681B

“Collected”
Handling Rules

- **To Enter,**
  - Ticket must have previously been in “Collected” State
  - Ticket Must Be Now Be In “Issued” State
- **To Exit,** Ticket Must Be In “Used” State
Exploiting This System

- What We Have Learned So Far
- System Safeguards
- Their Assumptions
- Attacks Against Their Assumptions
- Epic Fail!
What We Have Learned So Far

- **Object Based**
  - Physical Object
  - Database Object

- **Properties**
  - Identification
  - Type
  - Value
  - Location
What We Have Learned So Far

+ States
  + Issued
  + Used
  + Collected
+ History
System Safeguards

- Ticket Composition and Ticket Design
- Mirror Physical Object and Database Object
- Handling Rules Define Valid Use of The Objects
- Lifecycle limited to Twenty-Four Hours
- Collection of Ticket After Use
Their Assumptions

- No One Will Be Able to Reproduce Our Ticket
- Our System Has The Only Valid Objects
- Handling Rules Will Prevent Concurrent Use
- Damage is limited by Lifecycle
- After Use, Ticket Will Be In Our Possession
Attacks Against Assumptions

- Acquire Suitable Ticket
- Capture Valid Object
- Bypass Rules
- Extend the Attack to Increase the Damage
Epic Fail!

- Found Someone to Make Blank Tickets
- Copied Shit Ton of Objects in “Issued” State
- Found Flaw In the Handling Rules
  - “Collected” State found in Current Lifecycle
  - Overrides all other states!
- Object Always Seen Recently “Collected”
- Run The Original Ticket
- All Copies Immediately Become Valid
Epic Fail!
Epic Fail!
### Epic Fail!

<table>
<thead>
<tr>
<th>Date</th>
<th>Bahn</th>
<th>Station</th>
<th>Before Use</th>
<th>After Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/7/2018</td>
<td>15</td>
<td>Ari</td>
<td>0x00E0 0349083E 7826 0D2F7759 00FE74 00D20F 0D697408E8</td>
<td>0x00E0 0349083E 7826 0D2F7759 00FE74 00D20F 0D697408E8</td>
</tr>
<tr>
<td>10/7/2018</td>
<td>15</td>
<td>Ari</td>
<td>0x00E0 0349083E 7826 0D2F7759 00FE74 00D20F 0D697408E8</td>
<td>0x00E0 0349083E 7826 0D2F7759 00FE74 00D20F 0D697408E8</td>
</tr>
<tr>
<td>10/7/2018</td>
<td>15</td>
<td>Ari</td>
<td>0x00E0 0349083E 7826 0D2F7759 00FE74 00D20F 0D697408E8</td>
<td>0x00E0 0349083E 7826 0D2F7759 00FE74 00D20F 0D697408E8</td>
</tr>
<tr>
<td>11/1/2018</td>
<td>140</td>
<td>Sanam Pao</td>
<td>0x00E0 E9D64094 B846 262FF7C9 00FE F0 00820E 26317E1CC0</td>
<td>0x00E0 E9D64094 B846 262FF7C9 00FE F0 00820E 26317E1CC0</td>
</tr>
<tr>
<td>11/1/2018</td>
<td>140</td>
<td>Sanam Pao</td>
<td>0x00E0 E9D64094 B846 262FF7C9 00FE F0 00820E 26317E1CC0</td>
<td>0x00E0 E9D64094 B846 262FF7C9 00FE F0 00820E 26317E1CC0</td>
</tr>
</tbody>
</table>
Epic Fail! (Demonstration)
Turning The Exploit Into An Attack

- Tickets
- Plan
The Plan

- Buy Ticket (Daily Pass)
- Copy Ticket
- Use Original
- Hand Out Copies
- Have Fun!
- Repeat Tomorrow!
## Results of The Attack

**Extend the attack!**

<table>
<thead>
<tr>
<th>Attack</th>
<th>Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily Pass</td>
<td>Counterfeits</td>
</tr>
<tr>
<td>$140</td>
<td>$15</td>
</tr>
<tr>
<td>$140</td>
<td>$30</td>
</tr>
<tr>
<td>$140</td>
<td>$5,000</td>
</tr>
</tbody>
</table>

1 Month: $4,256,333 | $137,365.59 |
6 Months: $25,550,000 | $824,193.55 |
1 Year: $51,100,000 | $1,648,387.10 |
5 Years: $255,500,000 | $8,241,935.48 |
Avoiding Their Fate

- Test All Layers of a Solution
- Test for Application Issues
- Check Your Assumptions
- Use Compensating and Mitigating Controls
Links

+ https://www.youtube.com/watch?v=-uvvVMHnC3c
Links

+ https://www.msrdevice.com
+ https://www.alibaba.com/
+ https://nexqo.en.alibaba.com
+ http://www.nexqo.com/
+ https://www.bts.co.th/
+ http://www.btsgroup.co.th