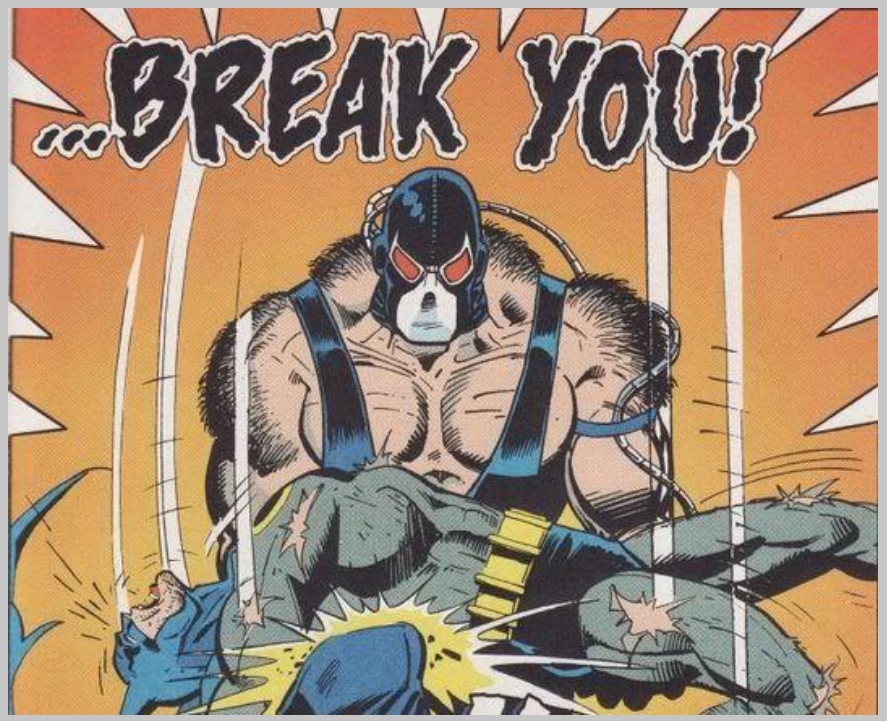
Breaking the back end!



DefCon 27, Las Vegas 2019

Hellfire Security

Gregory Pickett, CISSP, GCIA, GPEN
Chicago, Illinois

gregory.pickett@hellfiresecurity.com

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)

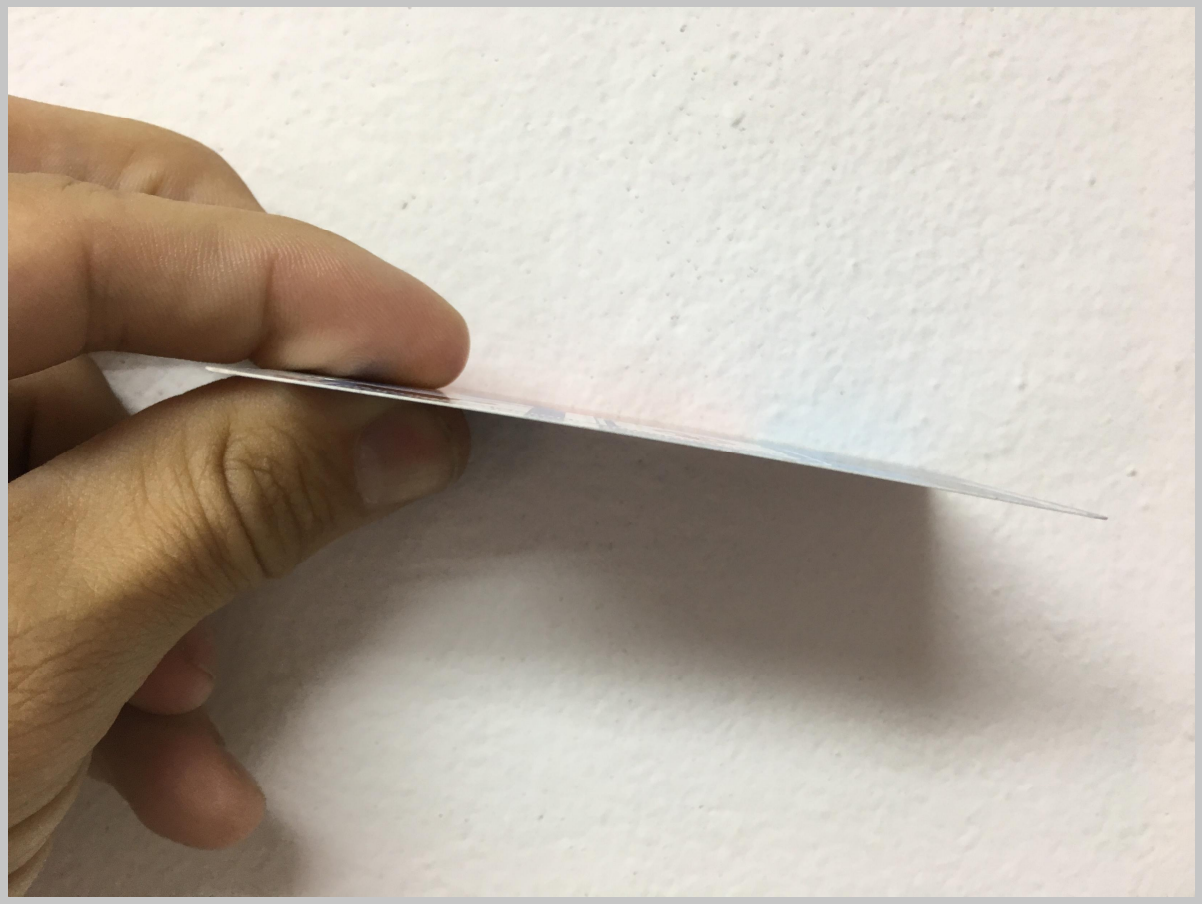
Tickets

- Two magstripes
- Hole through one magstripe
- Only 0.27mm thick

Tickets


สตรีมีครรภ์หรือผู้ที่จำเป็นต้องใช้ประตูพิเศษ
กรุณาติดต่อพนักงานนะครับ
Pregnant women, or other passengers
in need of assistance, please contact
BTS staff to enter or exit through
the swing gate.
ตั๋วโดยสารรถไฟฟ้าบีทีเอส ประเภทเที่ยวเดียว
BTS Single Journey Ticket

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

E0E64211A5 7826 FC2E843A 00FF74 00C20EFCE0933438

E0E64211A5 7826 FC2E843A 00FF74 00C20EFCE0933438

E0E64211A5 5826 E62E8E0A 00E0E64211A55826E62E8E0A

E0E64211A5 5826 E62E8E0A 00E0E64211A55826E62E8E0A

Start Sentinel

Duplicate

Known

Overwritten on Use

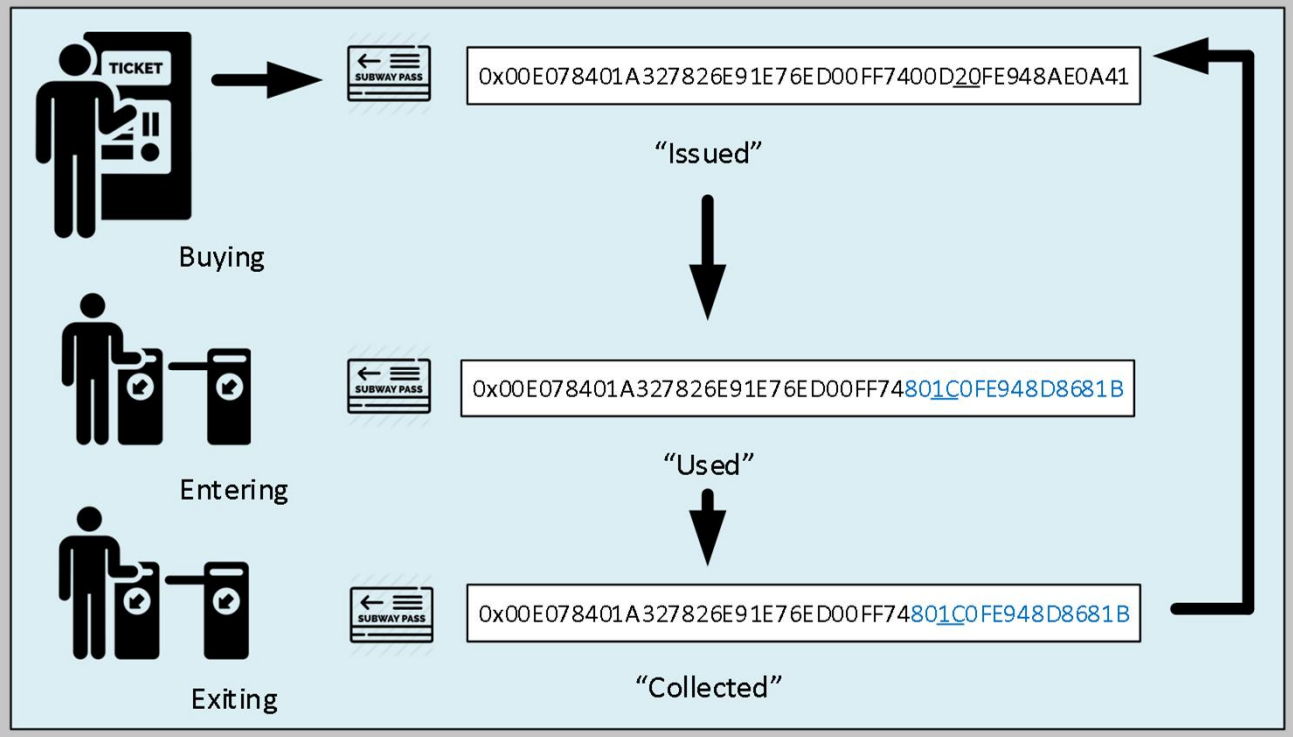
* The section “7826”” is the Ticket Type
* The section “00FF74” is always 100 + the price of the ticket
* For all day passes, the section “00FF74” is used to track trips taken

Field Work

Date	Baht	Station	GUID First		GUID			Second
2017	15	Ari	D0403AE7	F51CC51D	00D60F	F5A8 8 9A6C5		D01CCF12
2017	22	Ari	E0406C15	F52CD5A9	00D60F	F5A8 8 AA67B		E12CDD95
10/23/2017	16	Ari	A341760E	B02D364D	00D20F	B081 A 6087B		A42D3E71
10/23/2017	16	Ari	7A4101A9	B02DA6D4	00D60F	B081 A 72AC5		7A2DAE36
9/1/2018	16	Ari	78401A32	E91E76ED	00D20F	E948 A E0A41	801C0F E948 D 8681B	781C7D55
9/19/2018	16	Sanam Pao	E542D0B4	FB1EA6FC	00C20E	FBD8 8 D38D2		E51EAECA
9/20/2018	16	Sanam Pao	E64211A5	FC2E843A	00C20E	FCE0 9 33438		E62E8E0A
9/30/2018	16	Ari	32404A91	062FF509	00D60F	0631 D 72460		322CFF14
9/30/2018	23	Ari	FF421002	061F35FF	00D60F	0631 D 72498		001F3DD1
10/7/2018	16	Ari	03430838	0D2F7759	00D20F	0D69 7 408E8	801C0F 0D69 9 D6A2C	042F7F78
10/19/2018	140	Sanam Pao	E9D69E36	192FE79A	N/A	N/A	801C0F 19C9 D 5EA0A	E92EE6CF
11/1/2018	140	Sanam Pao	E9D64094	262FF7C9	00820E	2631 7 E1CC0	00060F 2631 E 58E52	E92EF6A3

Station Dispenser Station Turn-style

Field Work


TICKET
SUBWAY PASS
0x00E078401A327826E91E76ED00FF7400D20FE948AE0A41
"Issued"
Buying
SUBWAY PASS
0x00E078401A327826E91E76ED00FF74801C0FE948D8681B
"Used"
Entering
SUBWAY PASS
0x00E078401A327826E91E76ED00FF74801C0FE948D8681B
"Collected"
Exiting

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

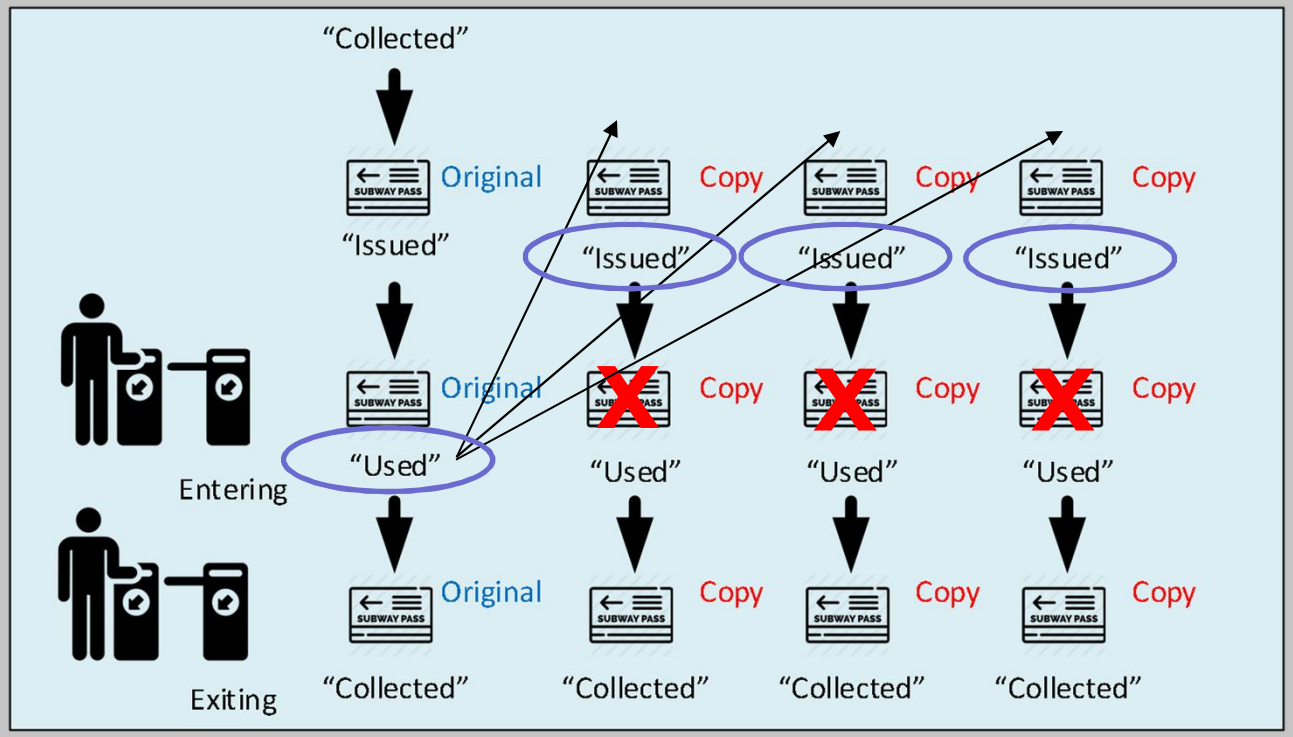
Attacks Against Assumptions

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

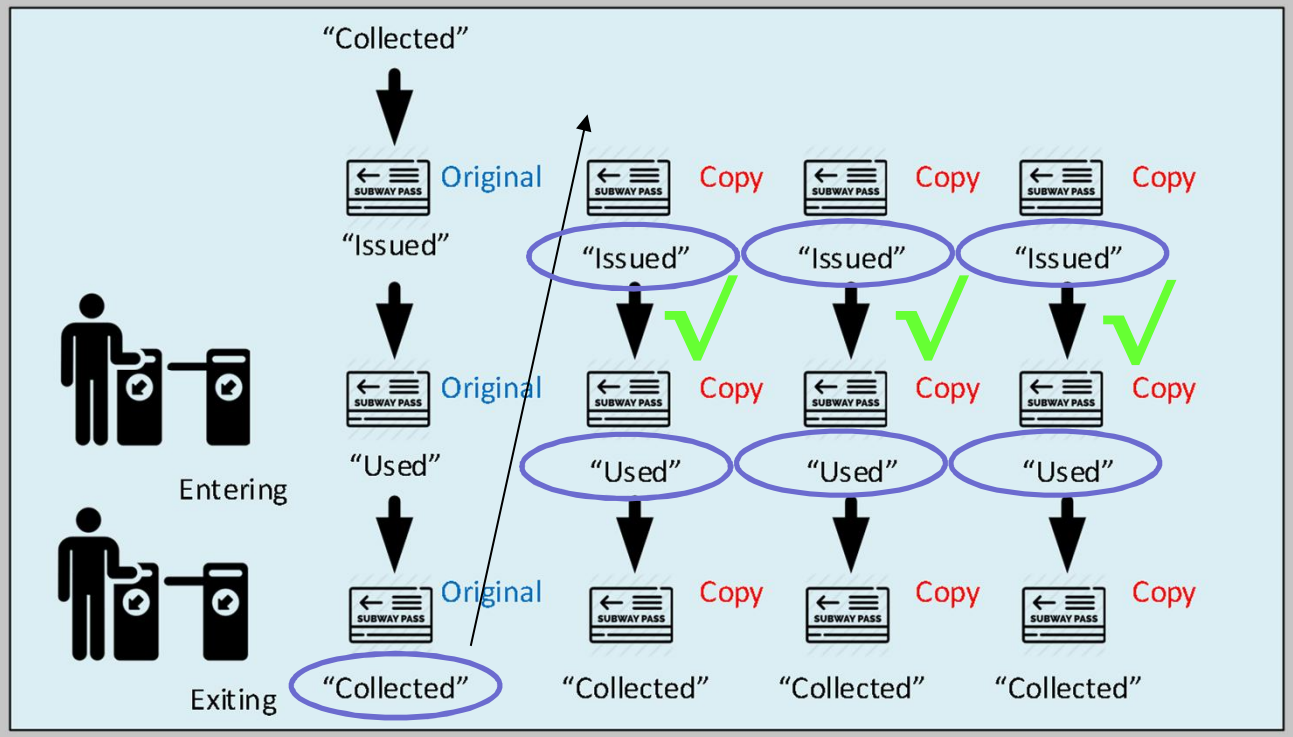
Epic Fail!

- 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!


"Collected"
Original
Copy
Copy
Copy
"Issued"
"Issued"
"Issued"
"Issued"
Original
Copy
Copy
Copy
"Used"
"Used"
"Used"
"Used"
Entering
Original
Copy
Copy
Copy
Exiting
"Collected"
"Collected"
"Collected"
"Collected"

Epic Fail!


"Collected"
Original
Copy
Copy
Copy
"Issued"
"Issued"
"Issued"
"Issued"
Original
Copy
Copy
Copy
"Used"
"Used"
"Used"
"Used"
Entering
Original
Copy
Copy
Copy
Exiting
"Collected"
"Collected"
"Collected"
"Collected"

Epic Fail!

			Before Use	After Use
			First Magstripe (Hole)	First Magstripe (Hole)
Date	Baht	Station	Track #1	Track #1
10/7/2018	16	Ari	0x00E0 03430838 7826 0D2F7759 00FF74 00D20F 0D697408E8	0x00E0 03430838 7826 0D2F7759 00FF74 801C0F 0D699D6A2C
10/7/2018	16	Ari	0x00E0 03430838 7826 0D2F7759 00FF74 00D20F 0D697408E8	0x00E0 03430838 7826 0D2F7759 00FF74 80040F 0D699F6834
10/7/2018	16	Ari	0x00E0 03430838 7826 0D2F7759 00FF74 00D20F 0D697408E8	0x00E0 03430838 7826 0D2F7759 00FF74 80040F 0D69D26878
11/1/2018	140	Sanam Pao	0x00E0 E9D64094 B846 262FF7C9 00FFF0 00820E 26317E1CC0	0x00E0 E9D64094 B846 262FF7C9 00FFEF 00060F 2631E58E52
11/1/2018	140	Sanam Pao	0x00E0 E9D64094 B846 262FF7C9 00FFF0 00820E 26317E1CC0	0x00E0 E9D64094 B846 262FF7C9 00FFEF 801C0F 2631E5EEA8

Epic Fail! (Demonstration)

Turning The Exploit Into An Attack

- Tickets
- Plan

Tickets

The Plan

- Buy Ticket (Daily Pass)
- Copy Ticket
- Use Original
- Hand Out Copies
- Have Fun!
- Repeat Tomorrow!

Results of The Attack

Attack				Damage		
Daily Pass	Counterfeits			Baht	US	
฿140	฿15		5	฿700	$	22.58
฿140	฿30		10	฿1,400	$	45.16
฿140	฿3,000		1,000	฿140,000	$	4,516.13
1 Month	฿4,258,333	$	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			

Extend the attack!

BTS GROUP

Avoiding Their Fate

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

Links

- https://wikileaks.org/wiki/Anatomy_of_a_Subway_Hack_2008
- https://file.wikileaks.org/file/anatomy-of-a-subway-hack.pdf
- https://defcon.org/images/defcon-16/dc16-presentations/anderson-ryan-chiesa/47-zack-reply-to-mbta-oppo.pdf
- https://www.computerworld.com/article/2597509/def-con--how-to-hack-all-the-transport-networks-of-a-country.html
- https://www.cio.com/article/2391654/android-nfc-hack-enables-travelers-to-ride-us-subways-for-free--researchers-say.html
- https://www.youtube.com/watch?v=-uvvVMHnC3c
- https://www.blackhat.com/docs/asia-17/materials/asia-17-Kim-Breaking-Korea-Transit-Card-With-Side-Channel-Attack-Unauthorized-Recharging-wp.pdf

Links

- https://www.msrdevice.com
- https://www.msrdevice.com/product/misiri-msr705x-hico-magnetic-card-reader-writer-encoder-msr607-msr608-msr705-msr706
- https://www.alibaba.com/
- https://nexqo.en.alibaba.com
- http://www.nexqo.com/
- https://www.bts.co.th/
- http://www.btsgroup.co.th


Q&A