RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: HTA-W02

That Point of Sale is a PoS

Charles Henderson
Vice President – Managed Security Testing
Trustwave
@angus_tx

David Byrne
Senior Security Associate
Bishop Fox

Agenda

- POS Architecture
- Breach Investigations
- Testing Techniques
- Penetration Test Findings

PoS Attacks: Theory vs. Reality

- Most breaches involve very simple vulnerabilities
- Future breaches are likely to leverage more complex vulnerabilities as merchants become more secure
- Many merchants have very immature security programs

PoS Purchasing: Security Is Not A Criteria

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Point of Sale Architecture

Hardware

- Standard PC workstation
- Specialized peripherals
  - Card reader and PIN pad
  - Barcode scanner
  - Touch screen – much less “specialized” than it used to be
  - Expanded keyboard
  - Scale
  - Customer display

Hardware

- Interfaces
  - USB
  - RS-232 – becoming less common
  - TIA-485/RS-485 – rare in 2015
  - Ethernet – some PIN pads and printers can connect directly to network

Client Operating System and Software

- Windows dominates
- Some Linux
- Occasional use of network boot with no local storage
- Even large retailers use off the shelf packages that are customized to the client

Application Servers

- Many separate systems:
  - Transaction records (purchases, refunds, etc.)
  - Payment card processing
  - Promotions
  - Customer tracking
  - Gift cards
- May be from entirely different vendors; more likely to see custom software in larger merchants

Application Servers

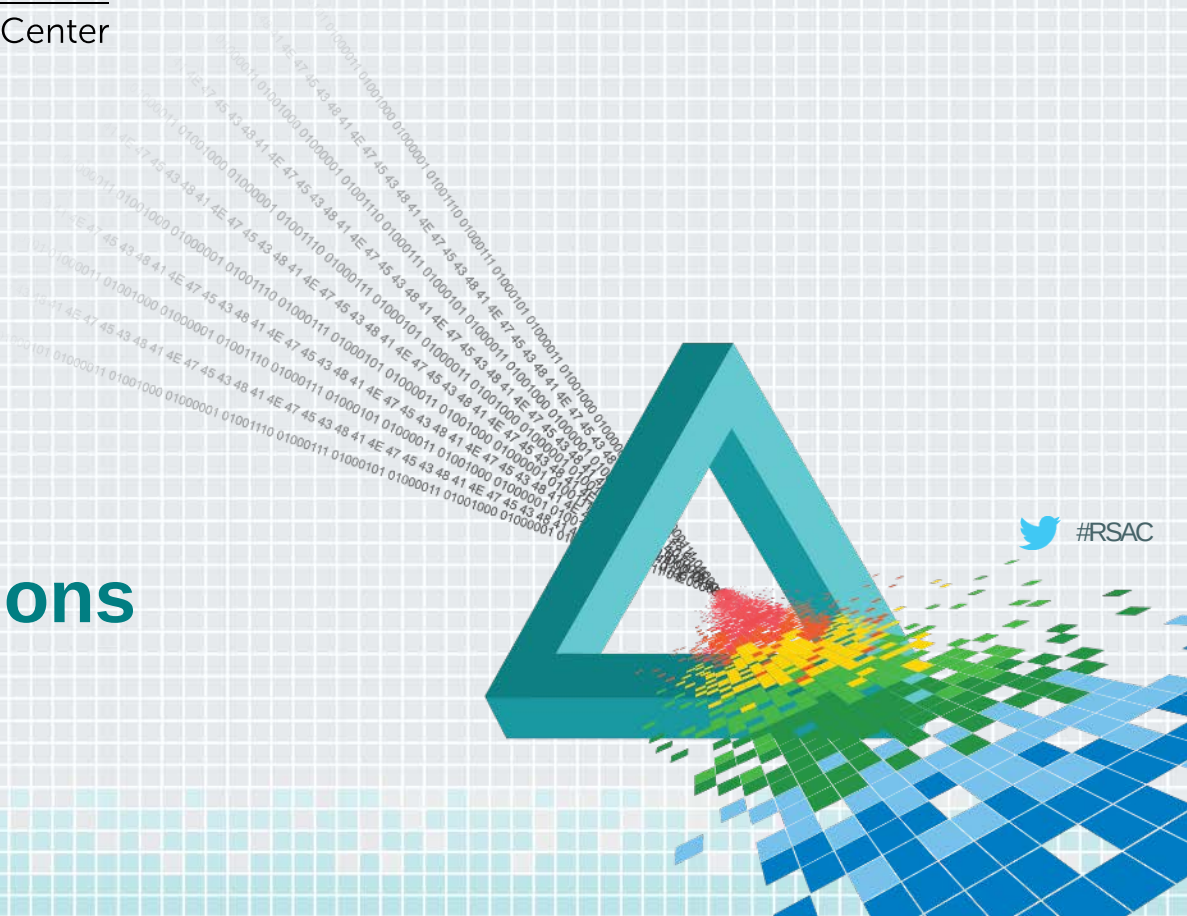
- In larger environments, typically implemented as middleware services: XML web services, etc.
- Small environments (isolated stores) likely to store all data on register.

Remote Administration

- Major source of compromise
- Registers will almost always have remote administration services
- Small organizations typically outsource administration
- Large chains will still not have on-site technical support

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Breach Investigations

Attacks Become More Efficient

- Physical Modifications (External)
- Physical Modifications (Internal)
- Drive-By Malware
- Scalable Malware

Physical Attacks (Internal)

Physical Attacks (Internal)

Physical Attacks (Internal)

Forensics Case Study One: Vendor Negligence

- Same administrator password for nine years
- Attackers most likely discovered merchant in breach of other merchant using same vendor

```
Username         : Administrator [500]
Full Name        :
User Comment     : Built-in account for
administering the computer/domain
Account Created : Xxx Xxx XX XX:XX:XX 2004
Last Login Date : Xxx Xxx XX XX:XX:XX 2013
Pwd Reset Date  : Xxx Xxx XX XX:XX:XX 2005
Pwd Fail Date   : Xxx Xxx XX XX:XX:XX 2014
Login Count      : 261
     Password does not expire
     Normal user account
```

Forensics Case Study Two: Vendor Negligence

- Attacker installs memory-scraping malware
- Data was *manually* retrieved by attacker; memory dumps left on PoS disk
- Malware easily discovered during investigation using current AV

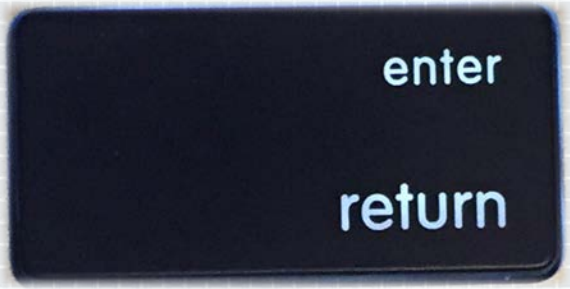
```
Scan type: Quick scan
Objects scanned: 191441
Time elapsed: 12 minute(s), 40 second(s)

Files Detected: 2
C:\WINDOWS\system32\Searcher.dll
(Trojan.Clicker) -> Quarantined and
deleted successfully.

C:\WINDOWS\system32\QOS.dll (Trojan.Agent)
-> Quarantined and deleted successfully.
```

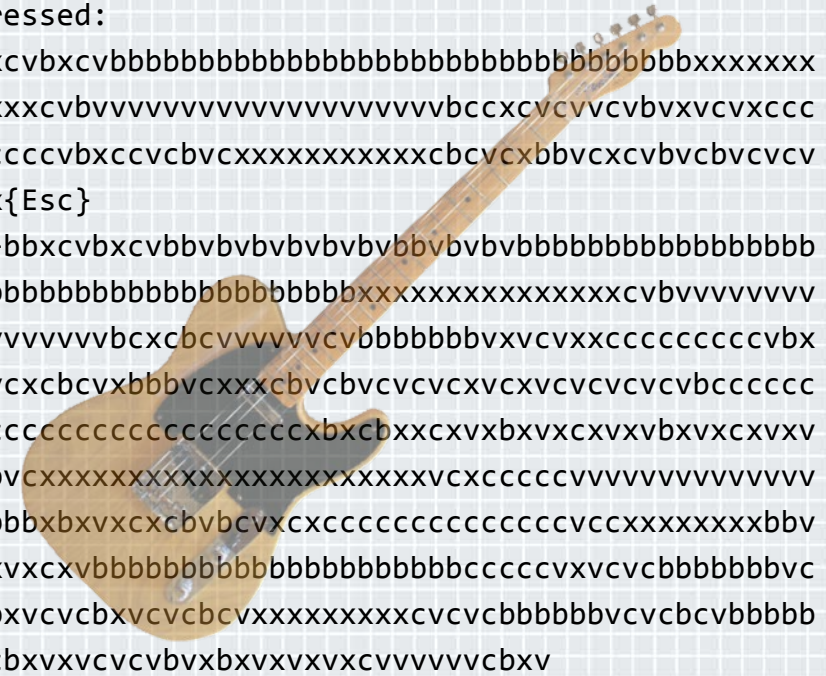
Forensics Case Study Three: Vendor Negligence

- Back of house server configured for remote management utilizing pcAnywhere
- Null Administrator password
- Administrator password had not been changed in nine years
- Malware easily discovered during investigation using current AV



Forensics Case Study Four: Origin of Malware

- Multiple workstations in CHD environment used to browse pornographic websites, download torrents, and video chat
- Keylogger installed by attacker also logged use of machines with CHD being used to play Guitar Hero 3, Call of Duty, and other games



Backoff Malware

- Self-propagates through weak remote access authentication
- Command and control features
- Memory scraping for payment card data
- Automatic data exfiltration
- Keylogging
- New infections look for old versions of Backoff to remove

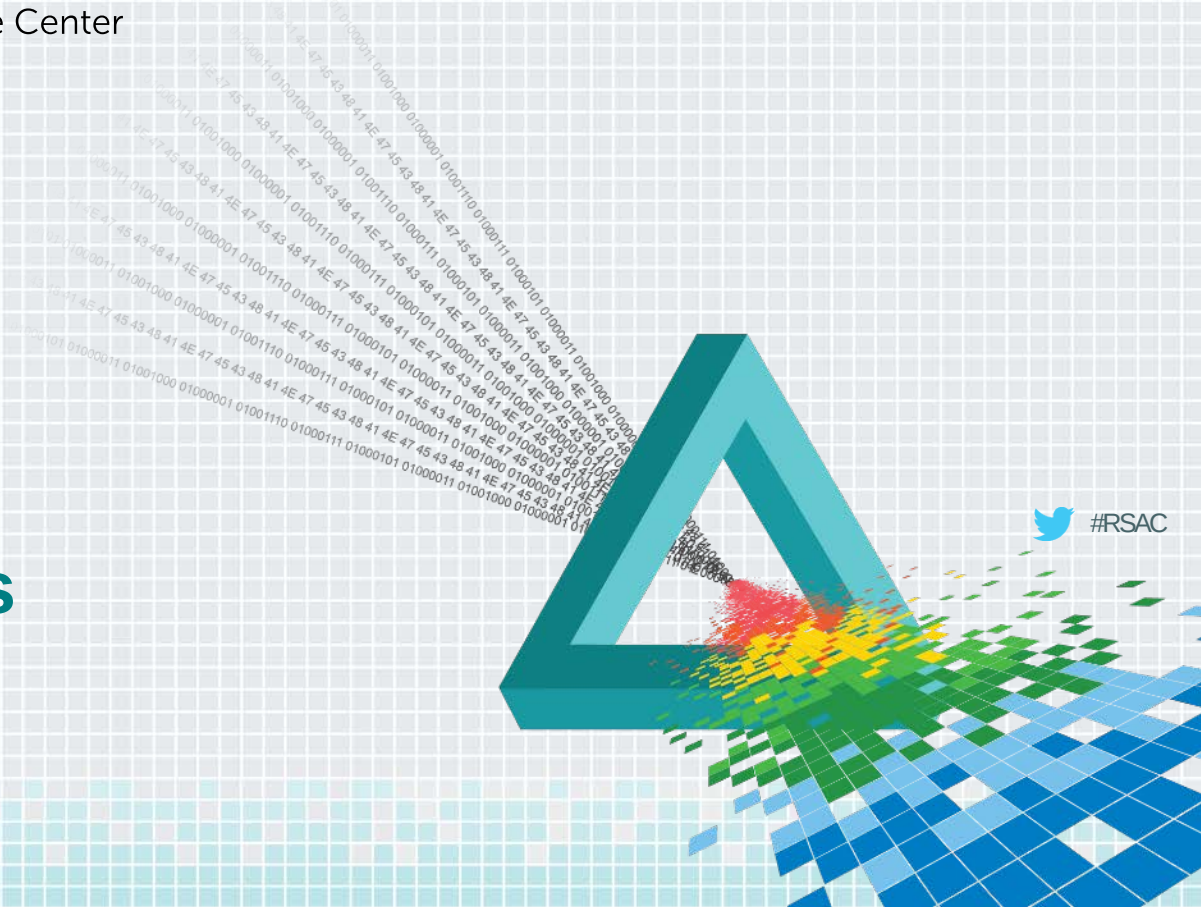
```
result = CreateToolhelp32Snapshot(2u, 0);
v1 = result;
if ( result != -1 )
{
  pe.dwSize = 296;
  result = Process32First(result, &pe);
  if ( result )
  {
    do
    {
      if ( !compare_exe_name(pe.szExeFile) && pe.th32ProcessID != current_pid && pe.th32ProcessID > 10 )
      {
        memory_scraping(pe.th32ProcessID);
        Sleep(10u);
```

```
for ( i = 0; i < maxAppAddr && VirtualQueryEx(pHand, i, &buf, 28u); i = buf.BaseAddress + buf.RegionSi
{
  if ( buf.Protect == PAGE_READWRITE && buf.State == MEM_COMMIT )
  {
    c = 0;
    while ( c < buf.RegionSize )
    {
      nSize = 0x100000;
      if ( buf.RegionSize - c <= 0x100000 )
        nSize = buf.RegionSize - c;
      rSize = 0;
      if ( ReadProcessMemory(pHand, buf.BaseAddress + c, lpBuffer, nSize, &rSize) )
      {
        c += rSize;
        find_track_data(lpBuffer, rSize);
      }
      else
      {
        c = buf.RegionSize;
      }
    }
  }
}
```

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Testing Strategies

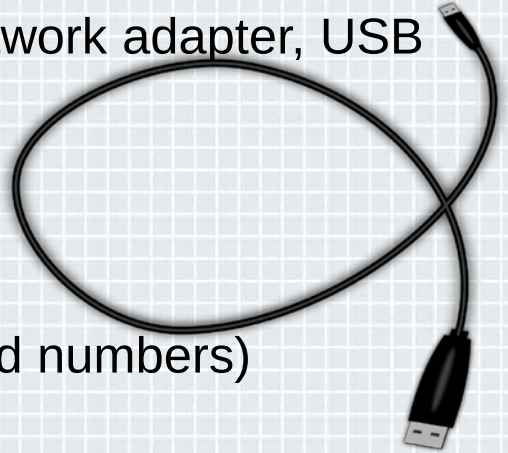


Multiple Testing Perspectives

- Remote (routed) network access
  - Vulnerable network services
- Local network access
  - Proper protocol encryption
  - Endpoint authentication (i.e., no MitM)
  - Identification of second-tier application servers

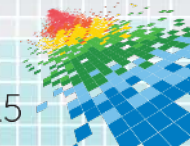
Multiple Testing Perspectives

- Momentary physical access
  - Introduction of malicious device – key-logger, network adapter, USB attacks, IEEE 1394 DMA, etc.
- Prolonged physical access
  - Hard drive encryption
  - Local storage of sensitive data (i.e., payment card numbers)
  - Analysis of application binaries
  - Monitoring and modification of key peripherals (i.e. PIN pad)



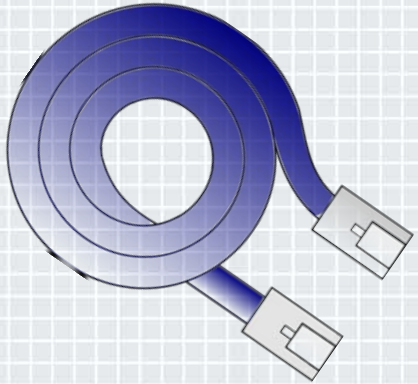
Multiple Testing Perspectives

- Console interaction
  - Execution of unauthorized and malicious programs
  - Escalation of system privileges
  - Modification of PoS application
  - Monitoring of network and peripheral communication
  - Memory dumps



Physical Security

- Quality of locks
- Exposed network cables, drops



RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Penetration Testing Results

Physical Security

- This is not good physical security
- Easy access to USB, Ethernet, etc

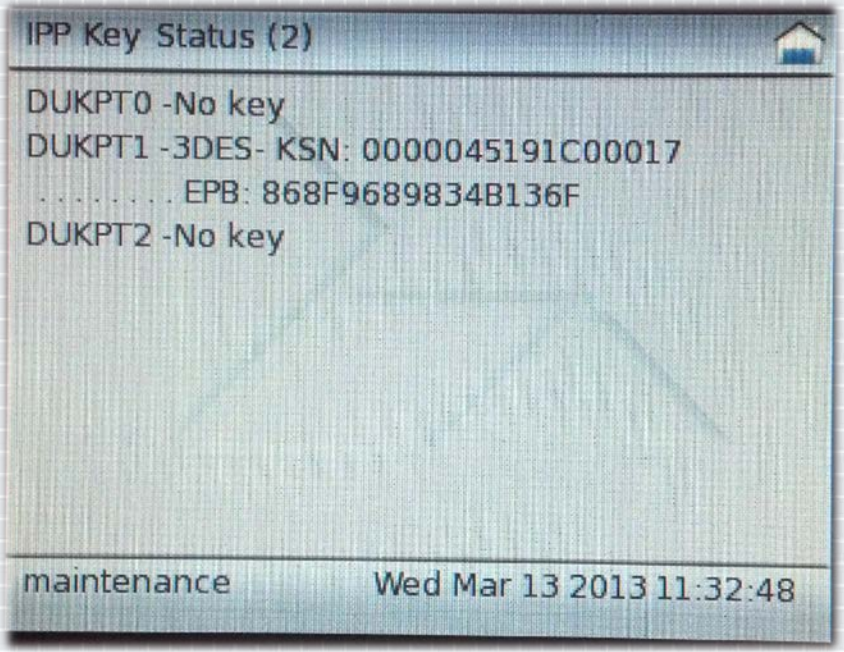
Physical Security

- This is not a good lock

166816 (Z66816)

- Since 1990, this has been the default password for all products from a major vendor
- Publically documented in a 1994 alt.2600 FAQ (featuring terms like “sysop” and company names like “Northern Telecom”)
- 90% of the terminals of this brand we test for the first time still have this code

Improper Use of Symmetric Keys



- Symmetric algorithms: one key for both encryption and decryption
- Asymmetric algorithms: decryption & encryption keys separate
- Using symmetric algorithms for payment card data invites abuse

Operating System Security

- Most POS deployments are overly reliant on passwords
  - Very difficult to secure OS passwords on endpoint
- AV scanning isn't perfect, but still important
- Easy to introduce custom malicious executables
- No drive encryption
  - Simplifies offline attacks
  - Allows stolen devices to be used for analysis
  - Devices get stolen

Authentication Fail

- Single set of authentication credentials across enterprise
- Automatic Windows login and local enforcement of POS user authentication – no authentication against networked application services

Running as administrator

- Vendors often claim that this is a requirement.
- Lies, nothing but lies.
- Windows and Unix-like operating systems have never worked this way.
- Simply an excuse for lazy programmers

```
08/14/2013 16:19:34:147 4011 3076 APP: *****Initializing Visual Payments Library****
08/14/2013 16:19:34:155 4011 3076 VPDATACAP: setSystemFunctionPtr - loaded libvfisvc.so library!
08/14/2013 16:19:34:156 4011 3076 VPDATACAP: setSystemFunctionPtr - obtained svcSystem() pointer 0x40424ef
08/14/2013 16:19:34:157 4011 3076 VPDATACAP: VPDATACAP library version is
08/14/2013 16:19:34:158 4011 3076 VPDATACAP: 00.00.17
08/14/2013 16:19:34:178 4011 3076 VPDATACAP: TCP_SYN_RETRIES is not in config.sys
08/14/2013 16:19:34:343 4011 3076 VPDATACAP: Getting terminals details such as IP address
08/14/2013 16:19:34:352 4011 3076 VPDATACAP: GetTermDetails - svcInfoPlatform(7) returned model=[870]
08/14/2013 16:19:35:307 4011 3076 VPDATACAP: Getting terminals details Done
08/14/2013 16:19:35:326 4011 3076 VPDATACAP: *VPSSL is not in config.sys
08/14/2013 16:19:38:651 4011 3076 VPDATACAP: InitVPOSLib - Socket ID=-1
08/14/2013 16:19:38:652 4011 3076 VPDATACAP: InitVPOSLib - Socket was not created.
08/14/2013 16:19:38:679 4011 3076 VPDATACAP: VPOFFLINESIGCOUNT is not in config.sys
08/14/2013 16:19:38:699 4011 3076 VPDATACAP: VPAUTOCLEARSIGINTERVAL is not in config.sys
08/14/2013 16:19:38:718 4011 3076 VPDATACAP: VPHEARTBEATINTERVAL is not in config.sys
08/14/2013 16:19:38:718 4011 3076 VPDATACAP: InitVPAppLib - APP VP Library initialized. Returning 1.
08/14/2013 16:19:38:719 4011 3076 APP: InitVPAppLib returned = 1
08/14/2013 16:19:38:720 4011 3076 APP: In writeAt
```

PIN Pad Debug Triggered

Trustwave

BISHOP FOX

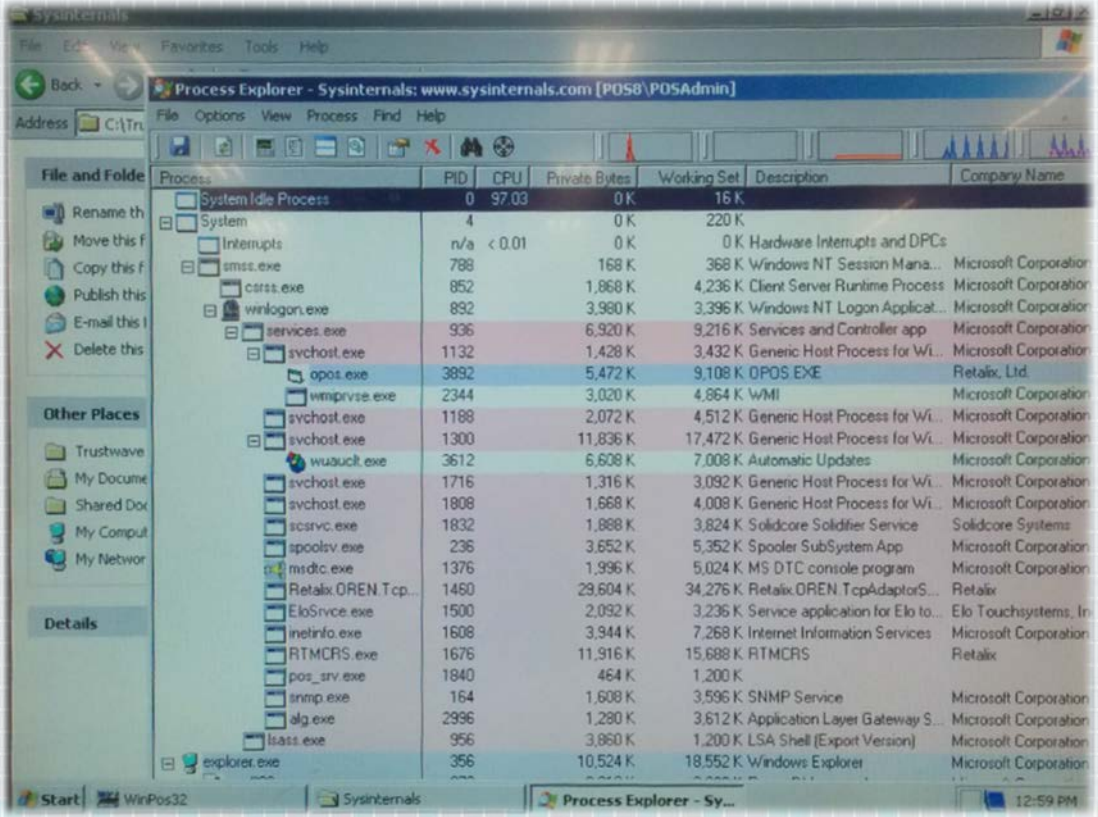

```
53791 619.1[illegible] Ibm_3d:f0:68  Ibm_3f:85:19     340 LLC      I, N(R)=56, N(S)=63
53793 619.15 Ibm_3d:f0:68  Ibm_3f:85:19      60 LLC      S, func=RR, N(R)=57
53794 619.15 Ibm_3d:f0:68  Ibm_3f:85:19      71 LLC      I, N(R)=57, N(S)=64

0000  00 1a 64 3f 85 19 00 1a  64 3d f0 68 01 46 e8 e8   ..d?.... d=.h.F..
0010  7e 70 08 00 01 00 3a 01  e2 03 09 00 04 a4 21 19   ~p....:. ......!.
0020  00 00 00 6a 01 00 00 02  35 00 00 00 00 00 00 36   ...j.... 5......6
0030  1e a2 0a 00 00 00 00 0d  01 00 00 0d 01 00 00 00   ........ ........
0040  00 00 00 20 20 20 20 22  99 3a 41 50 54 53 3a 30   ...    " .:APTS:0
0050  30 30 30 34 38 33 3a 53  50 54 53 54 76 44 45 53   000483:S PTSTvDES
0060  33 3a 61 4e 4f 53 50 3a  62 43 52 4d 43 3a 63 34   3:aNOSP: bCRMC:c4
0070  35 3a 64 32 35 34 34 34  30 30 39 39 39 39 32 32   5:d25444 00999922
0080  32 32 30 35 3d 31 34 31  32 31 30 31 30 30 30 30   2205=141 21010000
0090  30 37 31 37 30 30 3a 66  31 3a 67 32 32 3a 68 32   071700:f 1:g22:h2
00a0  33 30 33 32 3a 69 30 30  31 30 30 30 3a 6a 30 30   3032:i00 1000:j00
00b0  30 31 3a 6b 31 33 30 33  31 32 31 30 34 32 30 36   01:k1303 12104206
00c0  3a 6c 34 32 38 34 3a 6d  30 39 39 34 3a 6e 32 33   :l4284:m 0994:n23
00d0  30 33 32 3a 6f 32 33 30  33 32 3a 79 33 30 30 3a   032:o230 32:y300:
00e0  55 31 34 35 36 3a 35 31  33 30 33 31 32 31 30 34   U1456:51 30312104
00f0  32 30 36 30 32 30 30 30  30 31 32 38 34 32 31 38   20602000 01284218
0100  38 37 36 39 20 20 20 20  20 3a 7e 31 3a 28 41 3a   8769      :~1:(A:
0110  4e 3c 53 70 54 73 45 73  48 3d 30 30 30 44 3d 32   N<SpTsEs H=000D=2
0120  30 38 3e 38 37 31 46 31  38 34 37 32 44 46 38 31   08>871F1 8472DF81
0130  34 44 33 39 36 34 43 33  42 44 30 33 42 33 31 38   4D3964C3 BD03B318
0140  39 45 39 38 42 46 34 32  46 31 39 39 46 36 32 37   9E98BF42 F199F627
0150  42 22 0d 0a                                       B"..
```

Plaintext Network Traffic

Note the protocol. This is not IP.

Running Unauthorized Programs



- This is how malware infections start

Network Communication Security Flaws

- Plaintext communication
- Failure to authenticate endpoints
  - SSL is next to useless without certificate verification

Encryption Insanity

- Symmetric encryption used for transmission of payment cards
- Point-to-point-to-point encryption (one too many points)*
- XOR to protect passwords; programmers are always amazed that we can reverse this

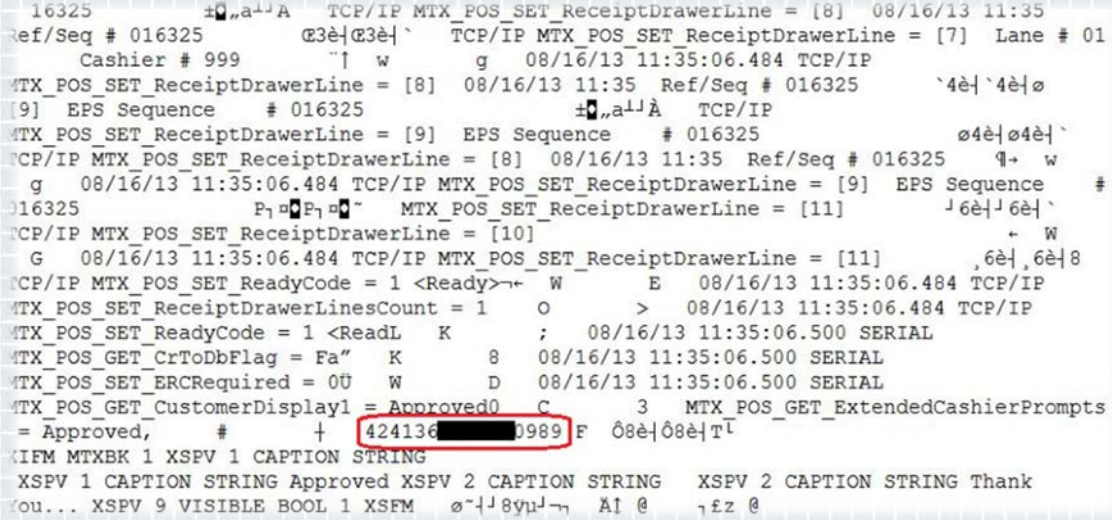
* Note: The addition of more points does not enhance security posture.

PIN Pad Security

- Default configuration often insecure
- Can almost always be reprogrammed from register
  - Convenient way of implementing management across enterprise
  - Some code is cryptographically signed
  - Configuration is almost never signed
  - Attacker may be able to disable security controls such as end-to-end encryption

PAN Abuse

- Coupon printer using PAN to track customers
- PAN returned to PoS for truncation
- Purchase history stored for tracking fraud – 37 million numbers
- Adding drives to register store growing debug transaction logs



Card Numbers in RAM

Symlink to Access Filesystem

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Apply:
PoS Security Program

Implement a PoS Security Program

- *Always verify the security claimed to be implemented by vendors*
- Top priorities:
  - Ensure no payment card data is stored on registers
  - Enforce strong authentication policies
  - Don’t run PoS user interface as “administrator”
  - Stay current on patches and AV signatures

Implement a PoS Security Program

- Secondary priorities:
  - Evaluate security of data communication (encryption, certificate checks, etc.)
  - Pen test application servers for application vulnerabilities
  - Lock down client execution environment
- Final efforts:
  - Use strong authentication (key/certificate-based)
  - Implement end-to-end encryption with asymmetric keys

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Q & A