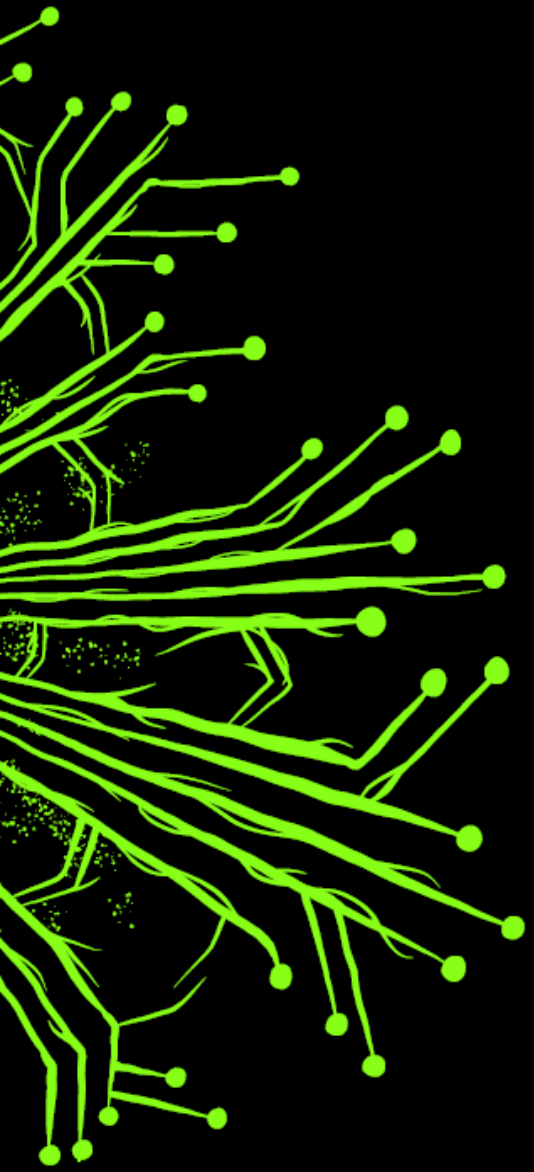


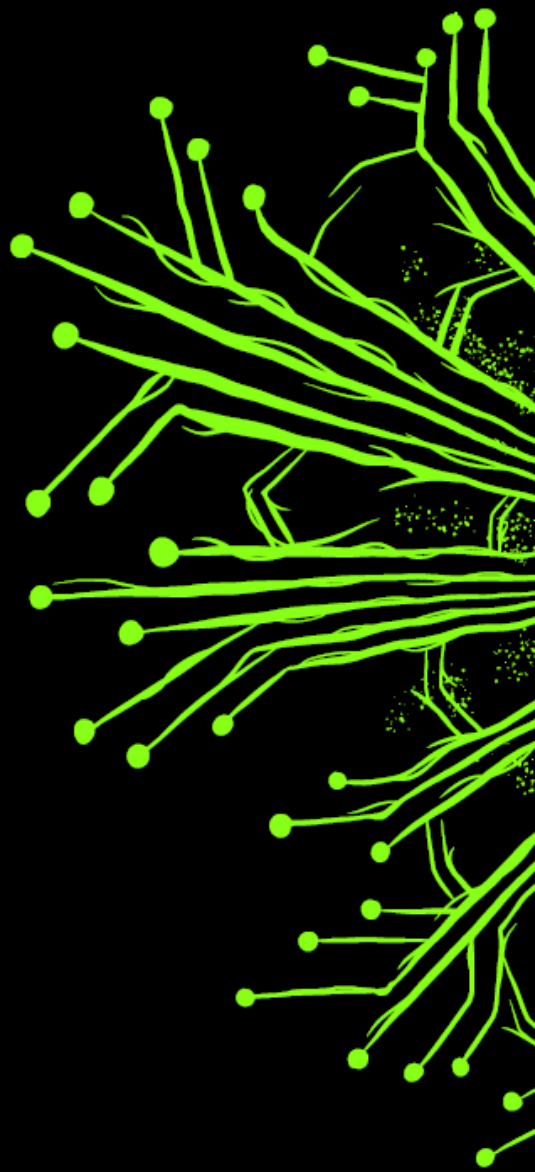
Point of Sale Hacking

You Sh0t the Sheriff 2.0

17 November 2008

Nicholas Percoco
Vice President, SpiderLabs

Trustwave®



Agenda

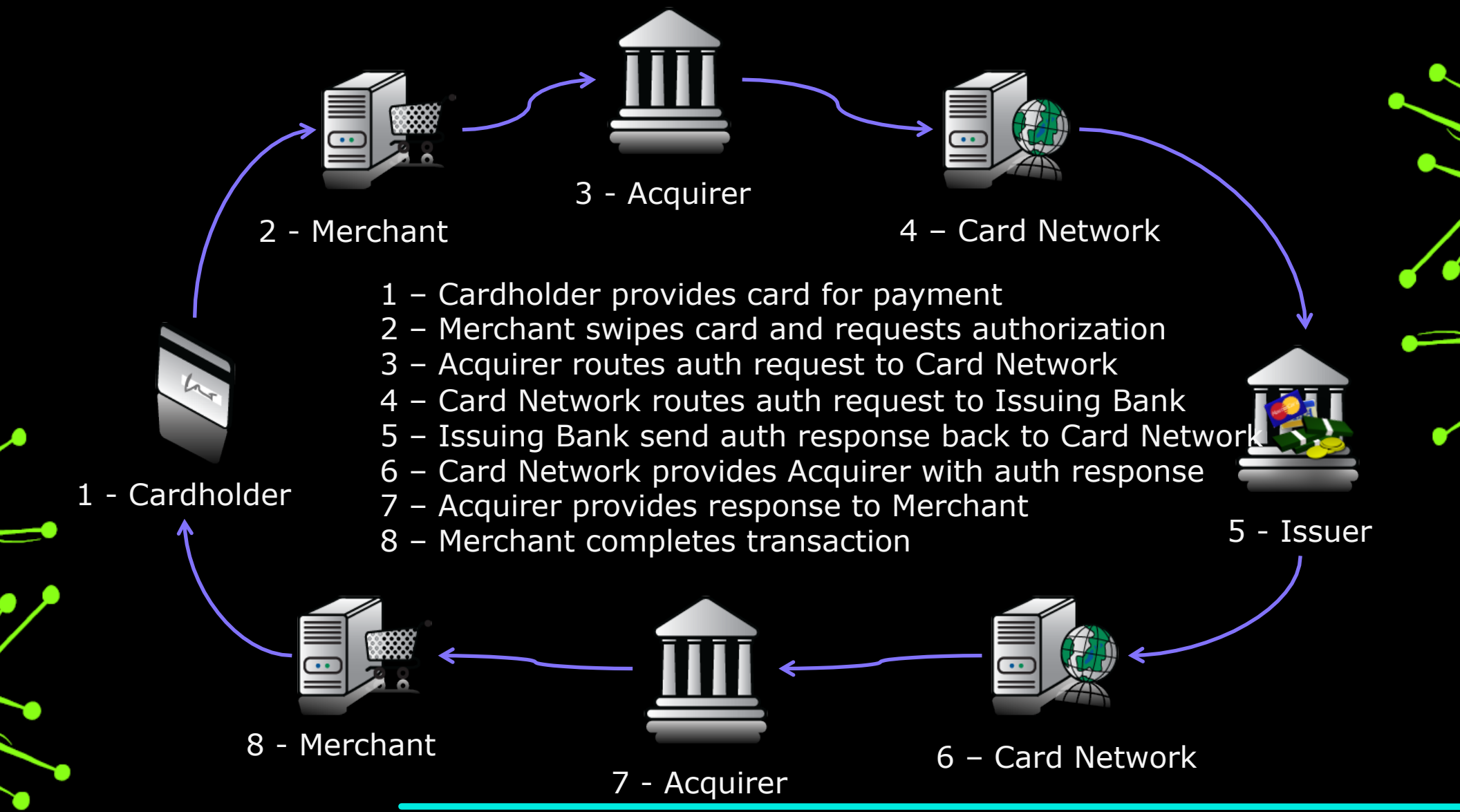
- About SpiderLabs
- Payment Processing Primer
  - Authorization
  - Settlement
- Point of Sale Architecture
- Common Weaknesses
- Account Data Compromise (ADC)
  - Defined
  - Data Types
  - Threats, Trends and Techniques
- Case Study
- Summary
- Questions

About SpiderLabs

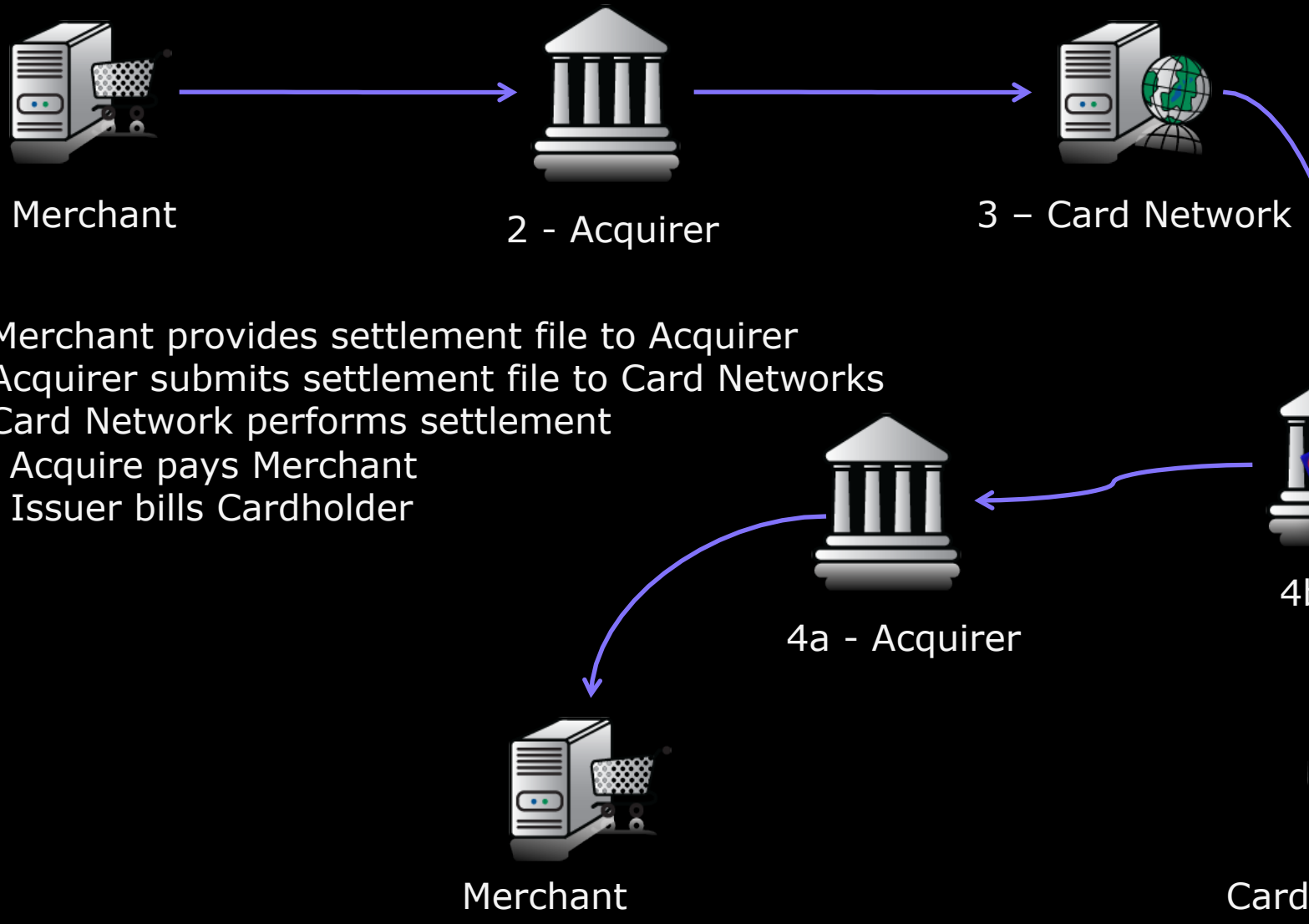
SpiderLabs is the advance security team at Trustwave responsible for incident response & forensics, ethical hacking and application security tests for Trustwave's clients.

SpiderLabs has responded to hundreds of security incidents, performed thousands of ethical hacking exercises and security tested hundreds of business applications for Fortune 500 organizations.

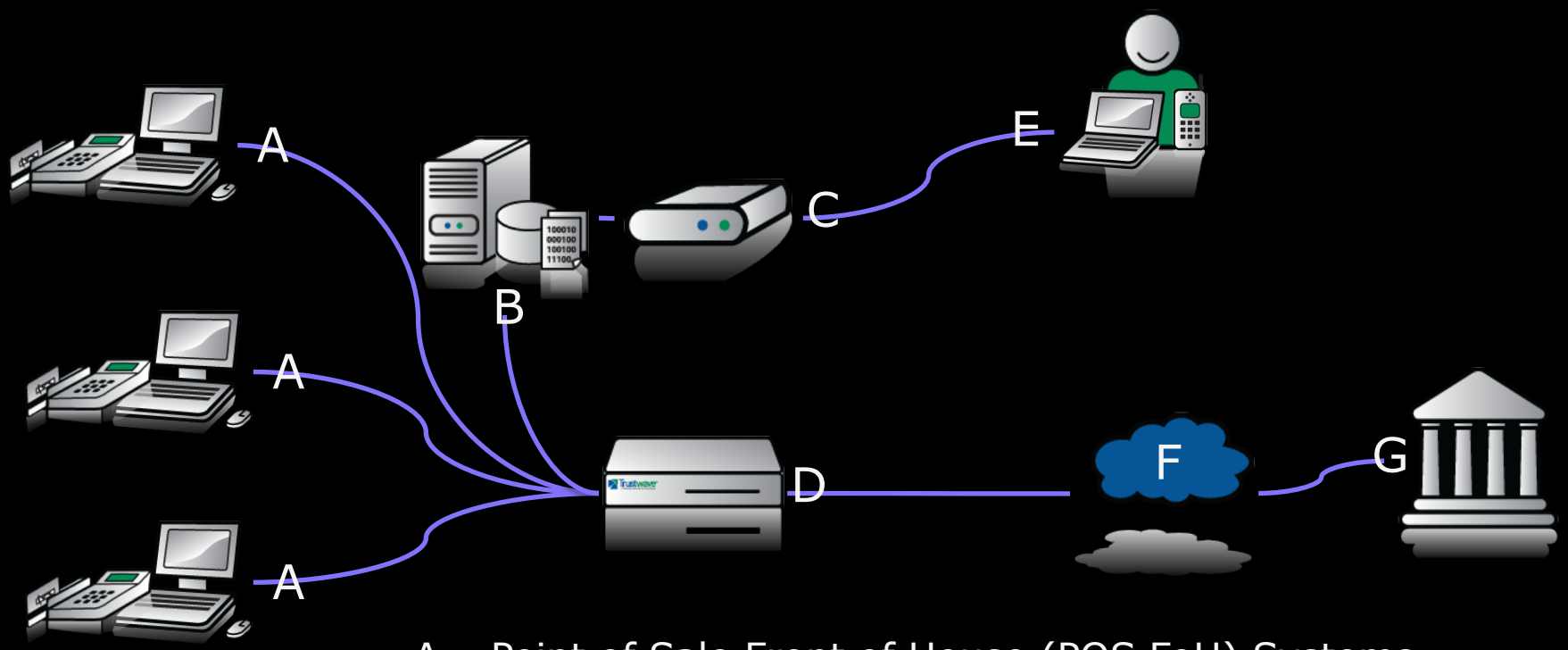
Payment Processing Primer - Authorization



Payment Processing Primer - Settlement

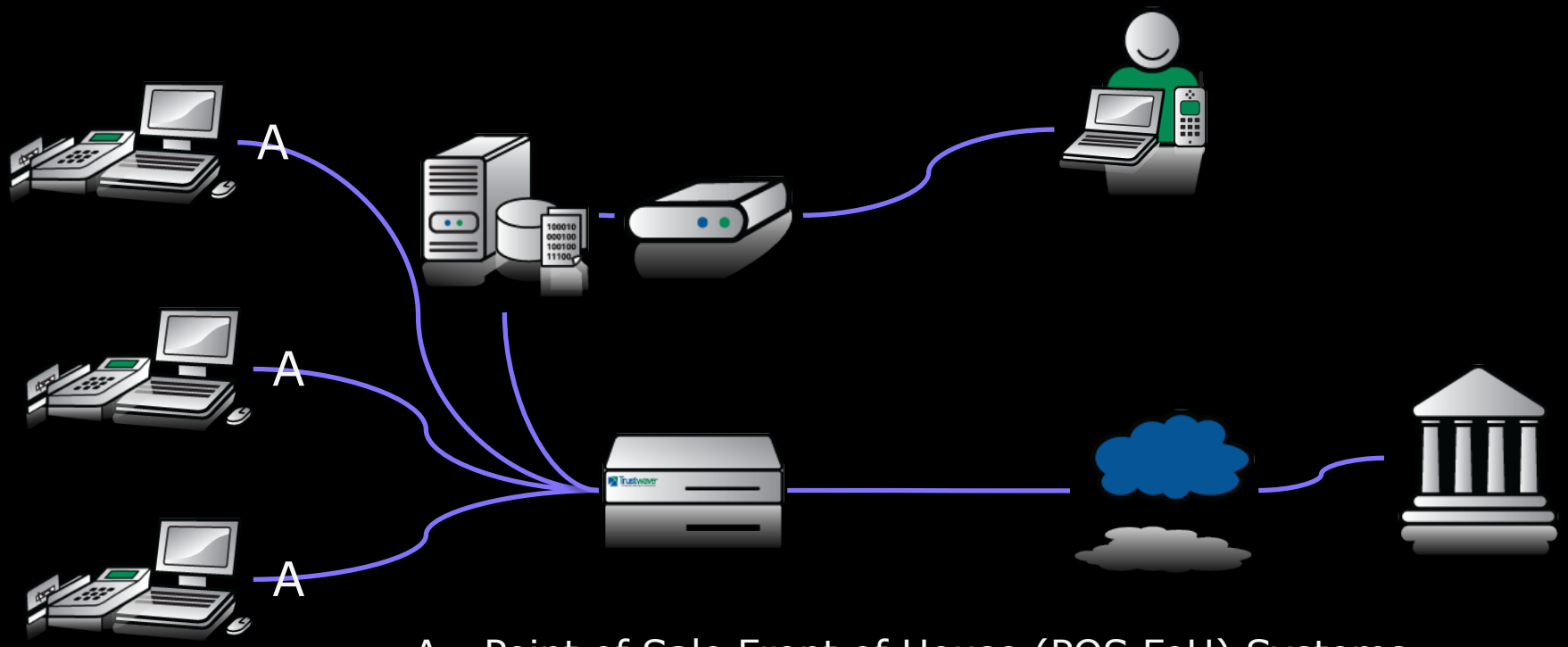


Point of Sale Architecture



A – Point of Sale Front of House (POS FoH) Systems
B – Point of Sale Back of House (POS BoH) System
C – Modem
D – Switch/Firewall/Router
E – Integrator/IT Support
F – Internet
G – Acquirer/Processor

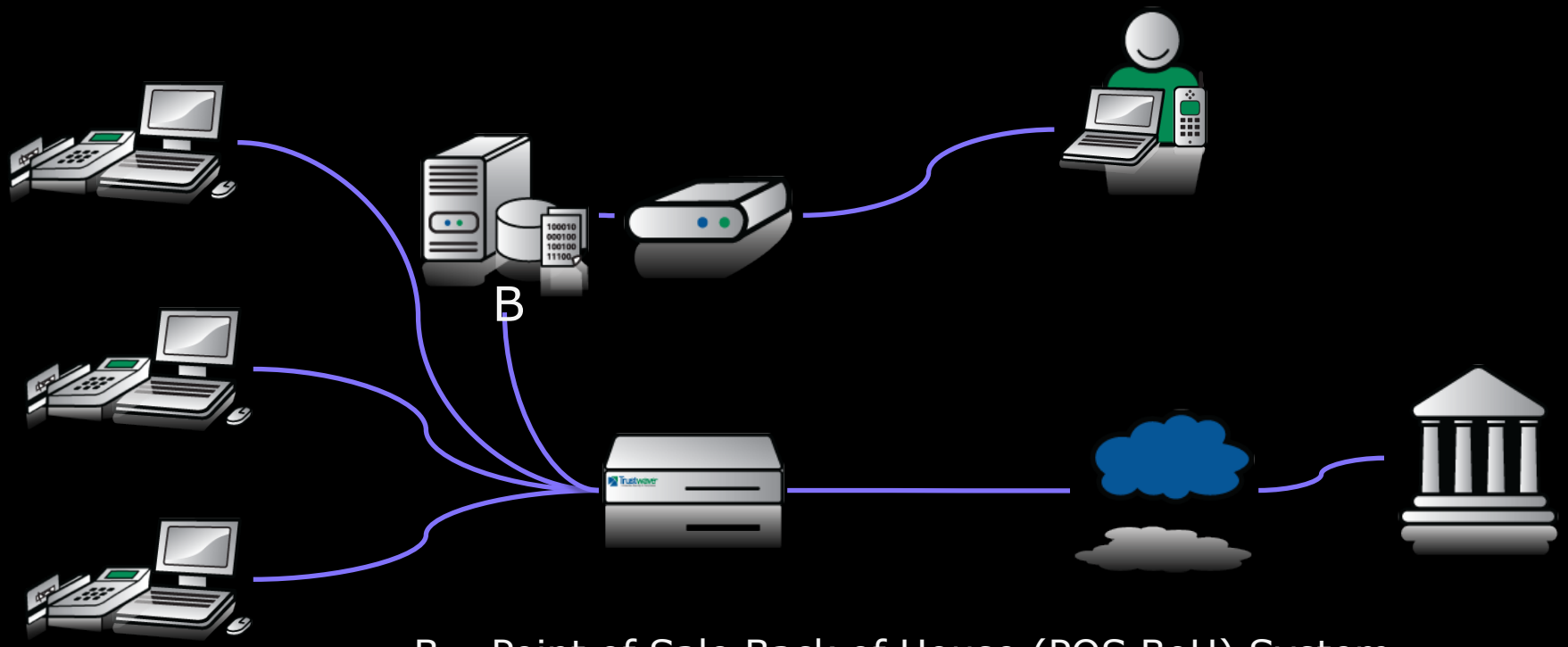
Common Weaknesses



A - Point of Sale Front of House (POS FoH) Systems

1. Typically PC-based
2. Auto-logon
3. Kiosk'd app on top of OS
4. RS-232 or USB card reader
5. No Antivirus
6. Default Passwords or Blank
7. Data sent to BoH in clear

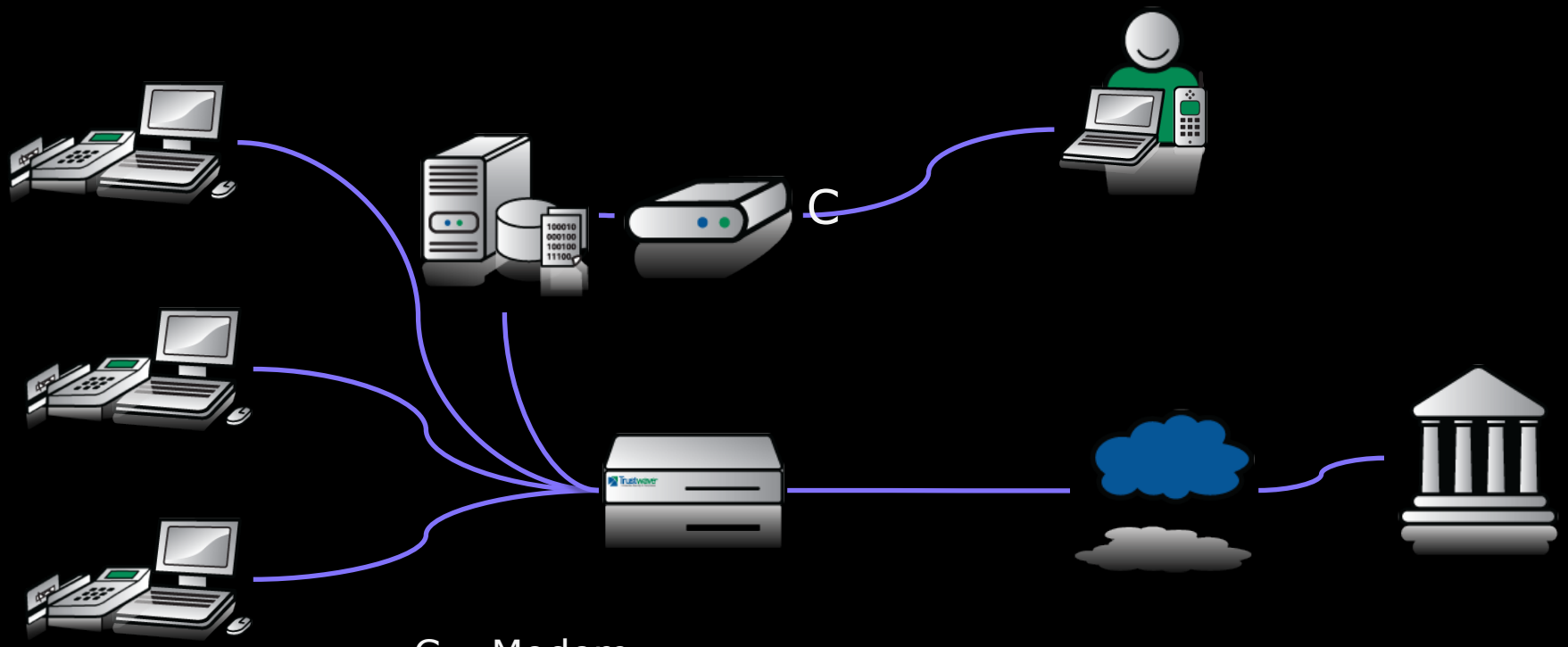
Common Weaknesses



B – Point of Sale Back of House (POS BoH) System

1. Typically PC-based
2. Often used as "office computer"
3. Remote Access Software
4. Simple Passwords
5. No "Auto Update"
6. No AntiVirus

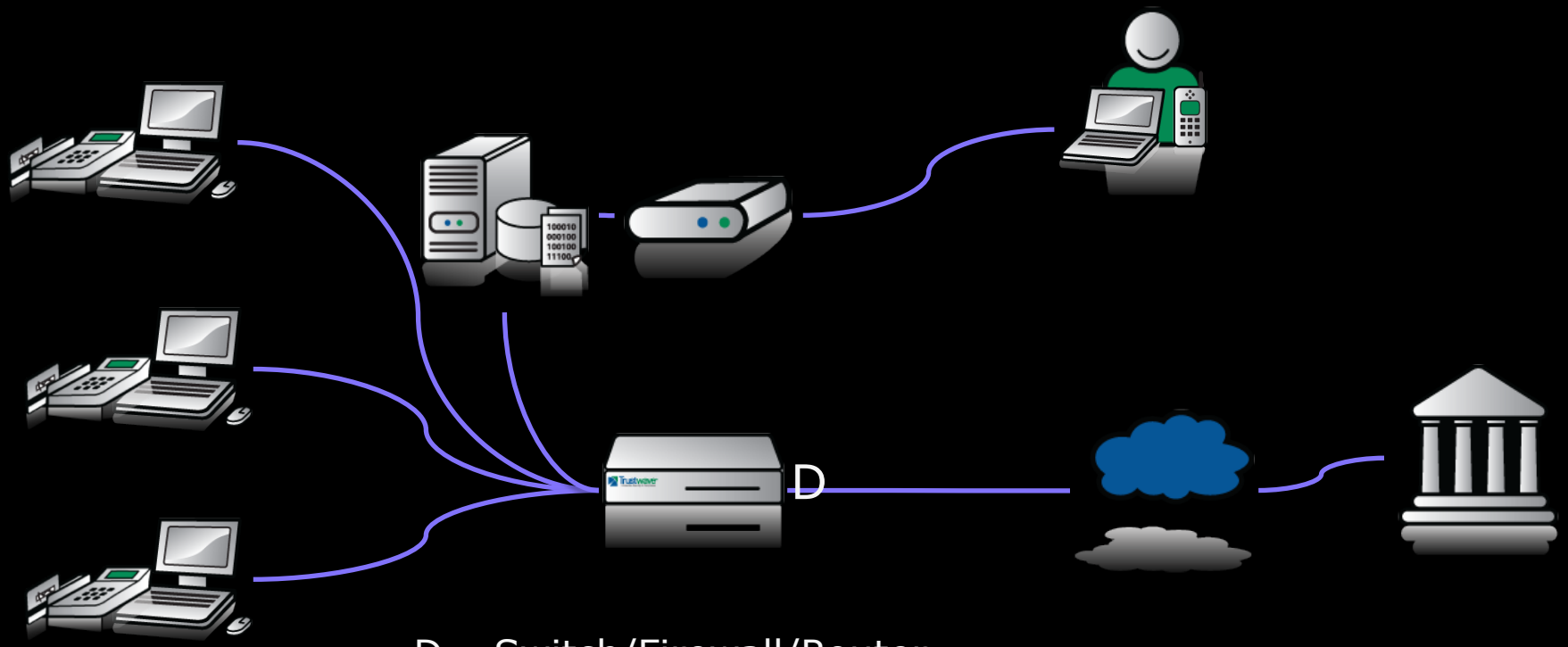
Common Weaknesses



C – Modem

1. Used for Remote Support
2. Auto Answer always On

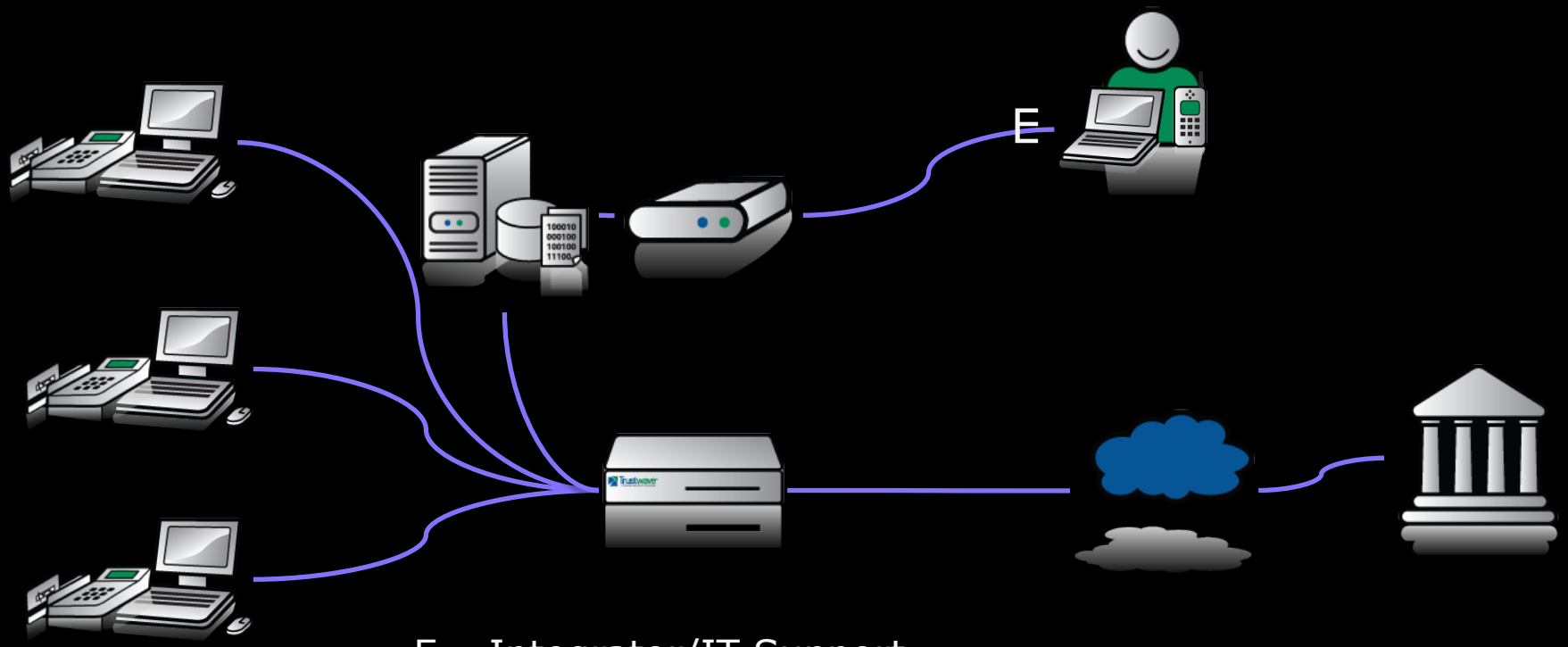
Common Weaknesses



D – Switch/Firewall/Router

1. Typically Consumer Grade
2. Default Configuration
3. Allows Remote Access ports Inbound
4. Allows all ports Outbound
5. Integrated Wireless Enabled, but not used…
6. No one watching the logs

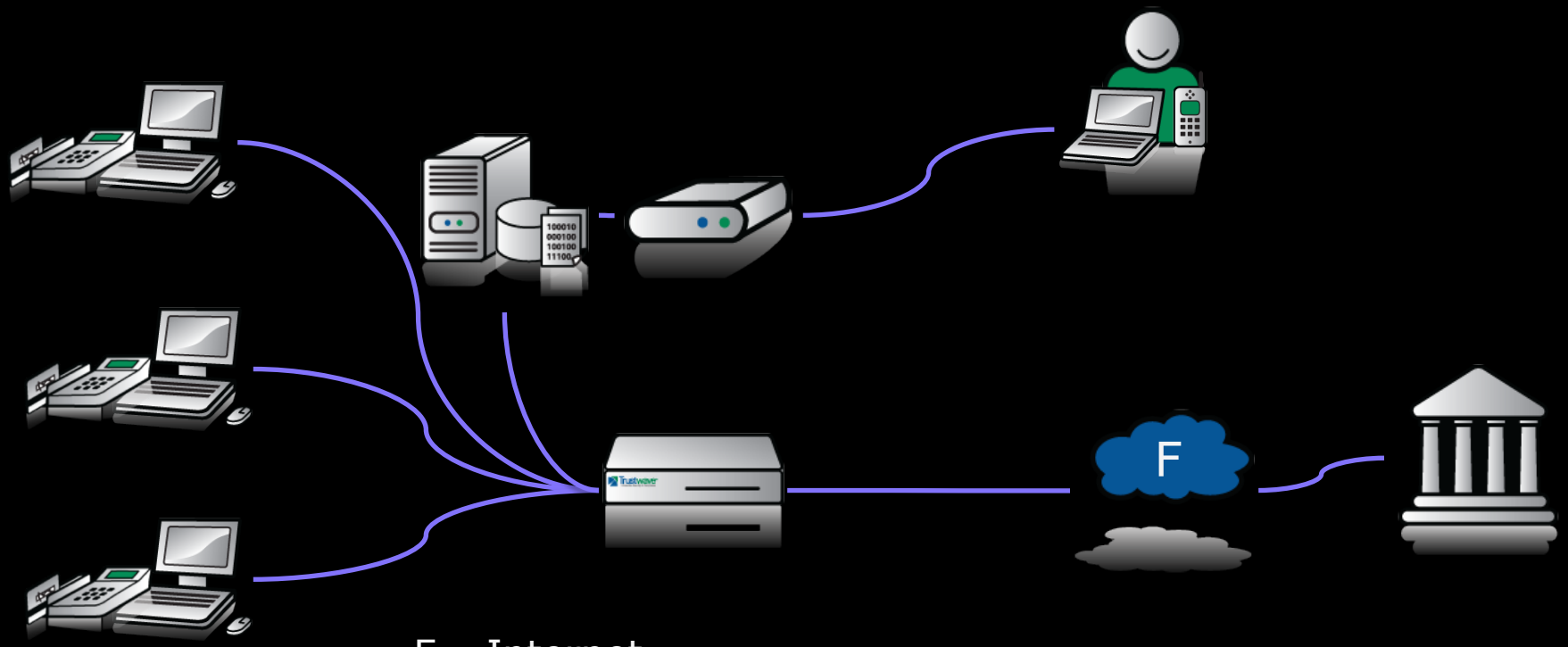
Common Weaknesses



E – Integrator/IT Support

1. No Security Experience
2. "Just get the job done!"
3. Shared password files (Excel)
4. Work from Home (access from home PC)

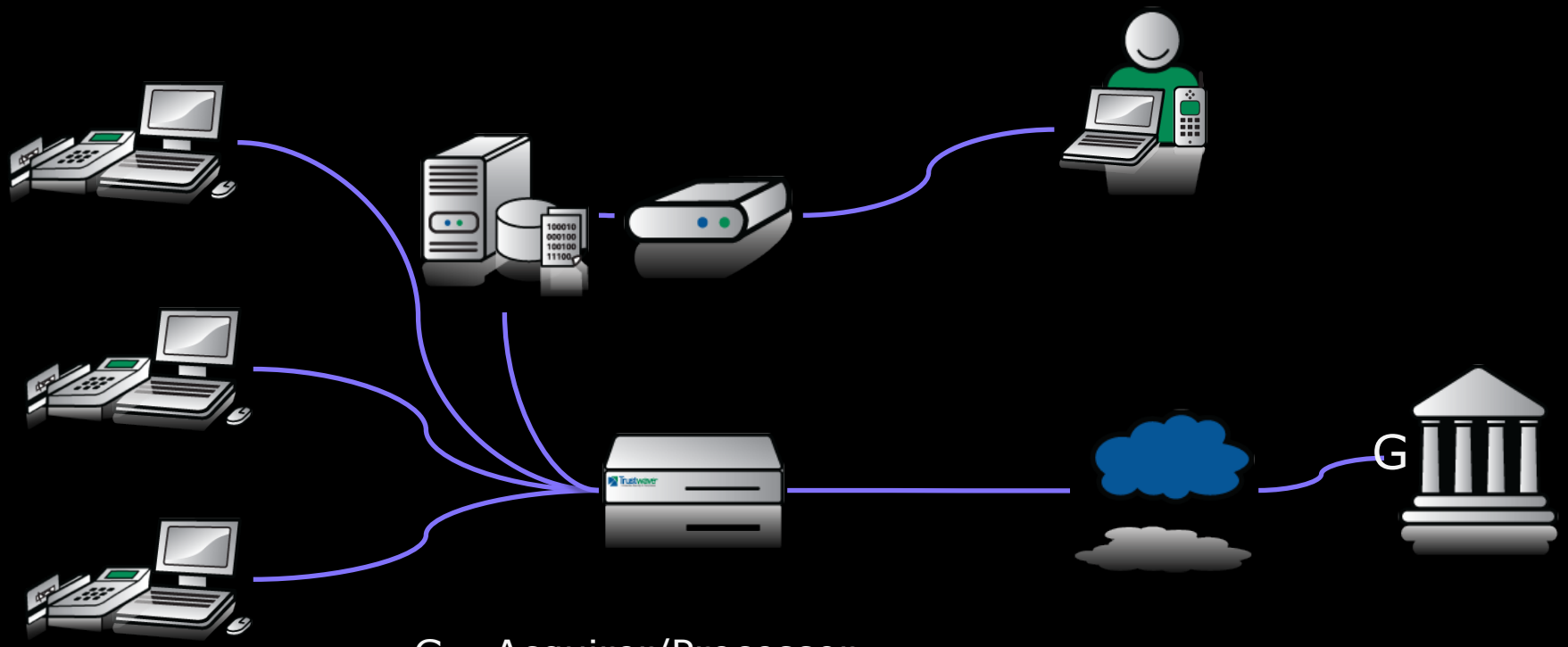
Common Weaknesses



F – Internet

1. It's Broken…
2. Clear text data can be intercepted

Common Weaknesses



G – Acquirer/Processor

1. Multiple Merchant's Data
2. Lack Security Budget
3. Web-based Merchant Portals
4. FTP for Offline/Batch Processing

Account Data Compromise - Defined

- A cybercriminal is an unauthorized individual or group taking advantage of a flaw or weakness within a computer system
- Today, cybercriminals are targeting systems that process, transmit, or store payment cards in order to obtain account information; this act is called an account data compromise
- To put thing simply, cybercriminals utilize tools to find gaps to obtain rewards

Account Data Compromise - Data Types

Card Present: Magnetic Stripe (Track) Data Targeted

Track 1: 76 Alphanumeric Characters

SS	FC	PRIMART ACCOUNT NUMBER	FS	NAME	FS	ADDITIONAL DATA	DISCRETIONAL DATA	ES	LRC

Track 2: 36 Alphanumeric Characters

SS	PRIMART ACCOUNT NUMBER	FS	ADDITIONAL DATA	DISCRETIONAL DATA	ES	LRC

Track 3: 104 Alphanumeric Characters

SS	FC	PRIMART ACCOUNT NUMBER	FS	ADDITIONAL DATA	DISCRETIONAL DATA	ES	LRC

Primary Data

SS: ***Start Sentinel***
FS: ***Field Separator***
ES: ***End Sentinel***
FC: ***Format Code***
LRC: ***Longitudinal Redundancy Check***
Primary Account Number: ***19 dig max***

Additional Data

Expiration Date (YYMM)
Service Code*
Country Code
Currency Code

Discretional Data

PVKI (PIN Verification Key Indicator)*
PVV (PIN Verification Value)*
CVV (Card Verification Value)*
CVC (Card Validation Code)*

*** Storage Prohibited post Authorization**

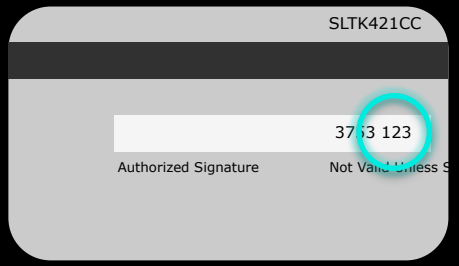
Account Data Compromise - Data Types

Card Not Present: Account Data + CVC Targeted

Card Validation Code is a 3 or 4 digit code printed on card

MasterCard ➔ CVC2 – Card Validation Coded
Visa ➔ CVV2 – Card Verification Value 2
Discover ➔ CID - Cardmember ID
American Express ➔ CID - Card Identification Digits

- Not included in Track Data
- Verifies possession of card
- Checksum for PAN
- Storage Prohibited post Authorization



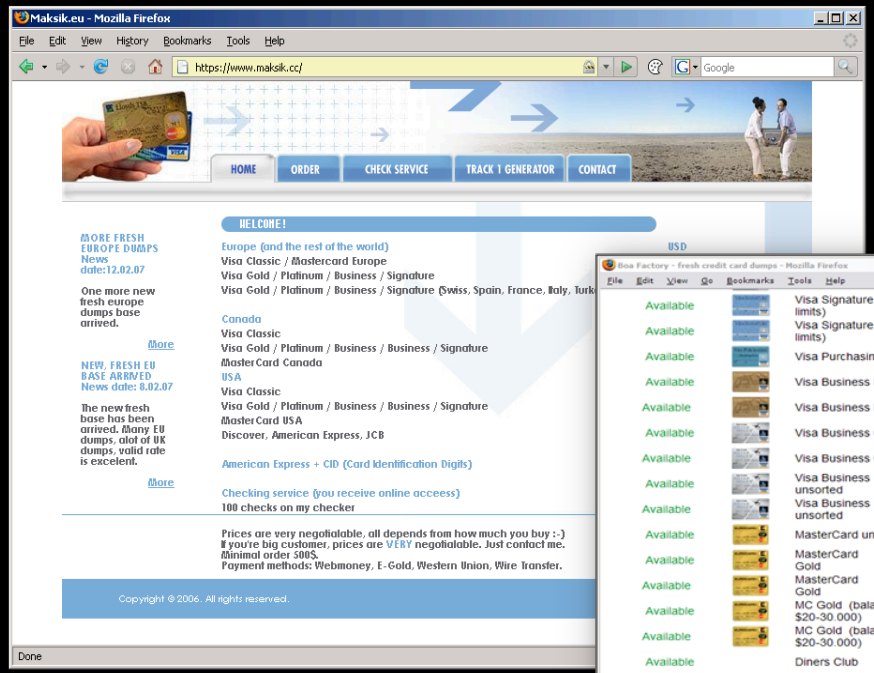
ADC - Threats, Trends and Techniques

Let's work backwards through this process…

Cybercriminals **Tools** **Gaps** **Rewards**

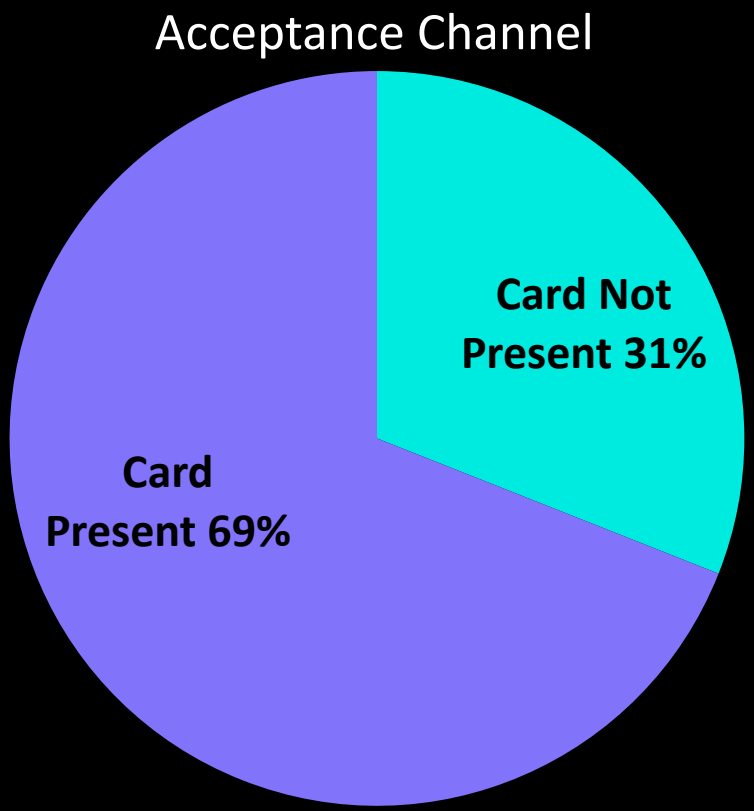
ADC - Treats, Trends and Techniques

Cybercriminals focus on financial gain!



ADC – Threats, Trends, and Techniques

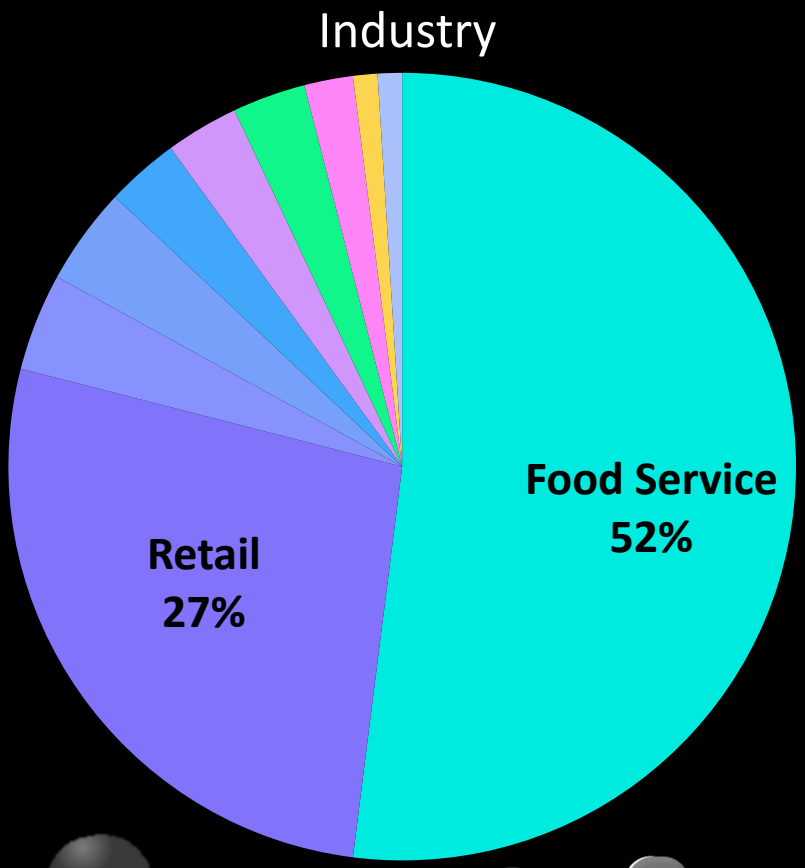
What 'gaps' are being found and exploited?



- Majority of Account Data Compromises investigated involved CP transaction
- 95% of CP compromised involved prohibited data storage
- Adoption of broadband Internet access continues to increase the pool of targets

ADC – Threats, Trends, and Techniques

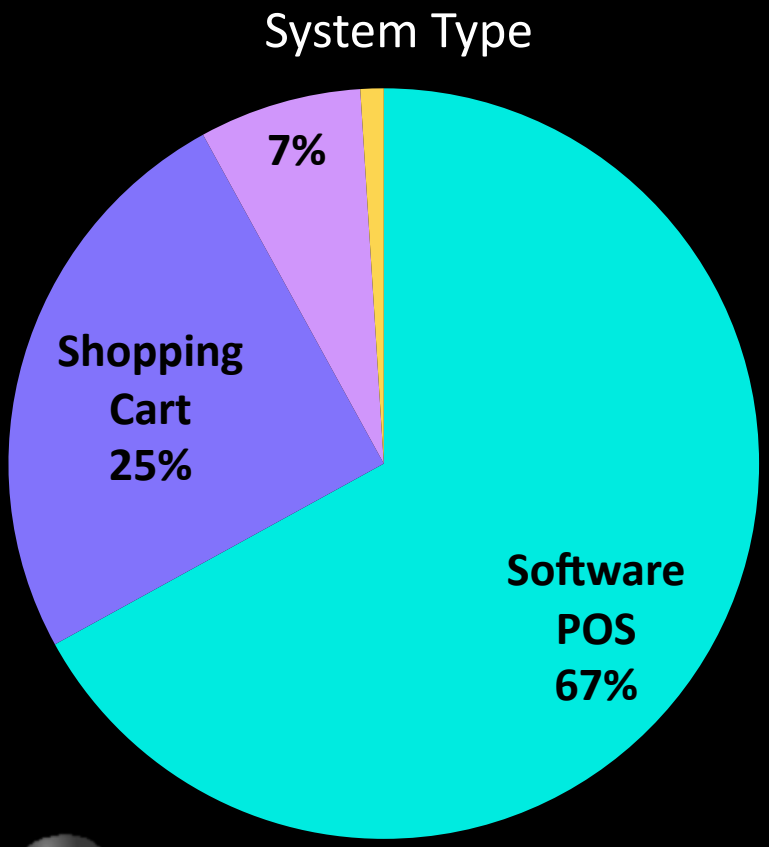
What 'gaps' are being found and exploited?



- Food Service and Retail industries commonly rely on 3rd party integrators
- Food Service and Retail generally not as aware of security as other industries; perimeter security often ignored

ADC – Threats, Trends, and Techniques

What 'gaps' are being found and exploited?



- **Software POS**: System that most often runs a PC-based operating system to accept CP transactions
- **Shopping Cart**: Web-based software utilized for eCommerce CNP transactions
- **Backend**: Centralized processing system often called a "transaction switch" to aggregate transactions from multiple POS
- **Hardware Terminal**: Dedicated device used by merchants in lieu of a Software POS system

ADC – Threats, Trends, and Techniques

What 'tools' are being used for CP compromises?

- Initial entry to Software POS commonly requires NO specialized tools due to improper perimeter security and the use of common desktop operating systems
- 3rd party remote access application almost always in use
- Access to native OS services as well (Windows Shares, RDP, SSH/Telnet)

How is unauthorized system access granted utilizing these services?

ADC – Threats, Trends, and Techniques

What 'tools' are being used for CP compromises?

Very Easily

- 3rd party integrators commonly utilize identical credentials for remote access applications for all clients
- Operating system credentials and settings are often **default** vendor-supplied and at times hard-coded
- Windows Terminal Services is often available and Administrator account can easily be brute-forced
- Vulnerabilities allow authentication bypass

ADC – Threats, Trends, and Techniques

What 'tools' are being used for CP compromises?

Once entry is granted, the attacker has a multitude of options to compromise account data

- Prohibited account data storage
  - Files simply uploaded
- Network Sniffers
- Keyloggers
- **Emerging Attack Vector:**
  - Custom POS Malware
- **Emerging Attack Vector:**
  - Parsing Volatile Memory

ADC – Threats, Trends, and Techniques

Who is involved with these account data compromises?

- Significant weight of attacks come from outside the US (China, Vietnam, Eastern Europe), although little indication whether this is the original source
- Utilizing network anonymity solutions (Tor Network) is increasingly common
- Speed of fraudulent accounts to market suggest criminal network is highly organized
- Apprehending cybercriminals is difficult given theft crosses international borders
- In the end, almost anyone could be involved

Case Study

Grocery Store Chain

- 14 locations identified as points of compromise by Visa
- Retail stores located throughout the US
- Accept debit and credit cards utilizing Software POS and PIN Pads
- Single 3rd Party Integrator supports all locations
- T1/DSL Internet conductivity at each location; no direct conductivity between retail locations

Case Study

Findings

- Attacker entered systems through remote access application utilized for 3rd party integrator support
- Installed network packet sniffer on the Back of House Server, although traffic between POS registers and Back of House server was encrypted
- Subsequently jumped to POS registers and installed serial port sniffer to capture account data traversing between PIN pad and POS register – Success!
- Uploaded account data daily via remote access application; undetected for over 3 months

Case Study

How are all 14 disconnected, geographically-dispersed locations compromised with 1 hour?

Analysis revealed remote access system files contained stored credentials & locations (IP) for all 14 locations…

…and additional credentials & locations for 350+ clients of the 3rd party integrator

Case Study

Outcome

- Additional 50+ stores were identified as points of compromise by Visa
- Millions of dollars lost in fraud
- 3rd Party Integrator held liable by merchants; loss of business
- Involvement of United States Secret Service

Summary

- Skill set required is minimal
- Attackers utilize common methods and tools
- Food service and retail industries pose the greatest risk in the US
- Remote access solutions present a huge problem for POS Systems
- Most compromises can be avoided by following basic security guidelines and compliance requirements

Questions?

Nicholas J. Percoco
Vice President, SpiderLabs
Email: npercoco@trustwave.com
Phone: +1 312 873-7471

Thank You!