RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

SESSION ID: SPO-R02

Crypto-Segmentation: Protecting Networked Applications When Firewalls Fail

Satyam Tyagi
Chief Technology Officer
Certes Networks
CertesNetworks.com
@CertesNetworks

Adam Boone
Chief Marketing Officer
Certes Networks
CertesNetworks.com
@CertesNetworks

They are already inside … we just have not found them

Security Crisis: Outdated Architecture

Borderless Enterprises

Apps digitized, extended outside firewall, rise of Shadow IT

Firewalls Fail

Access for working = access for hacking

Segmentation Chaos

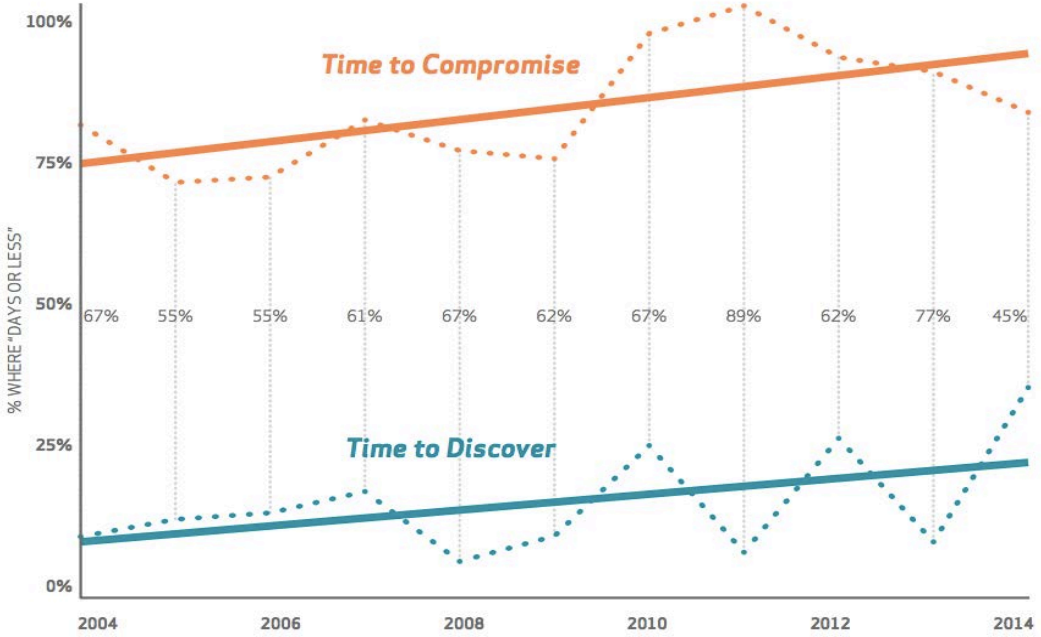
SSL, TLS, IPsec, VPN, DMZs, VLANs, ACLs

Performance hits

Gaps & trade-offs

Impact: Data Breach Crisis

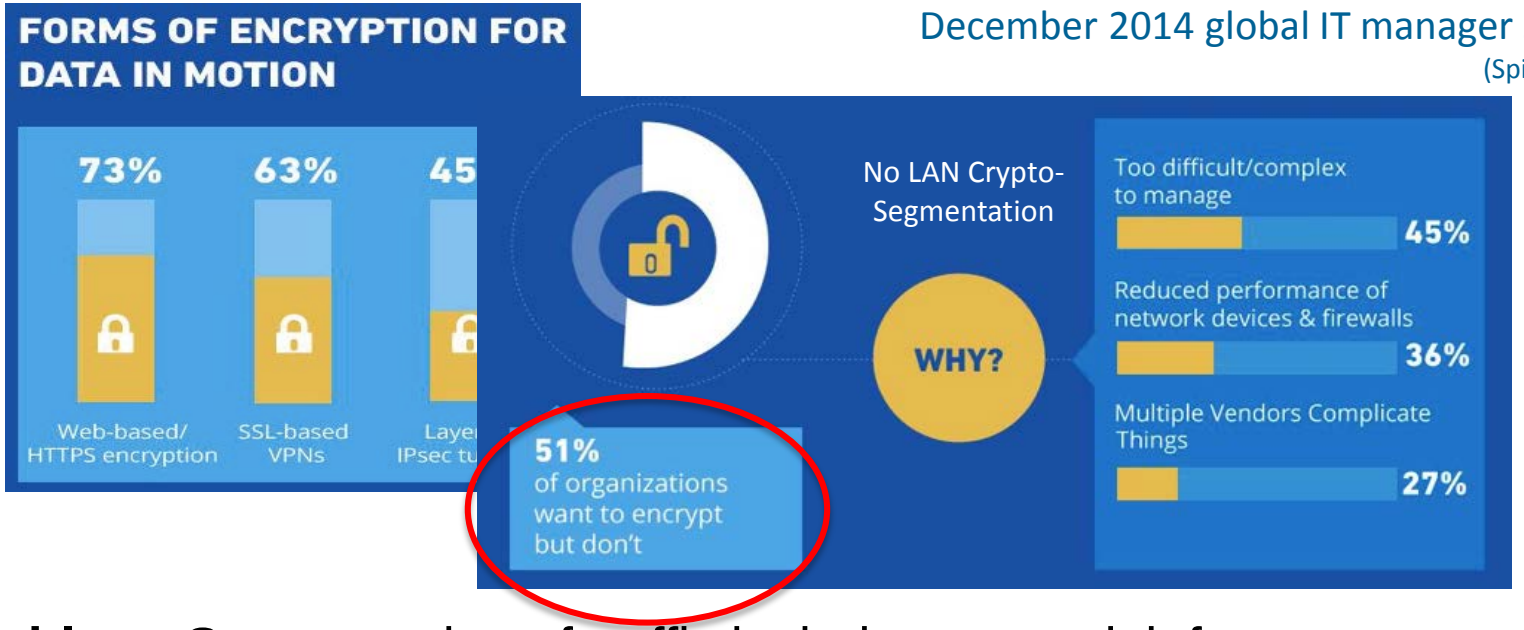
- In 60% of cases, attacker compromise organization in minutes
- 75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours)
- Breach discovery is days or weeks



The “Post-Trust” World

- No internal network can be fully trusted
- No user can be fully trusted
- Assume the breach has already happened
- Architecture based solely on perimeter security (firewalls, IDS/IPS) to keep the bad guys out is obsolete
- Common strategy is to use network segmentation

The Dirty Secret of Network Segmentation

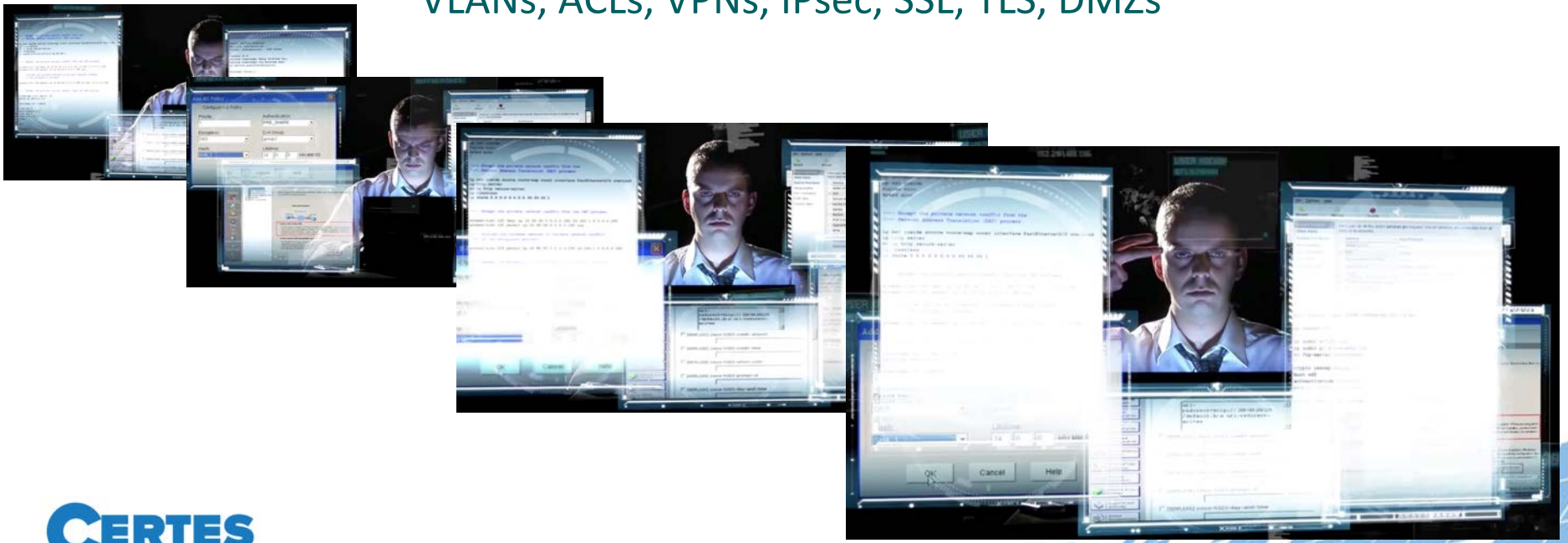


December 2014 global IT manager survey
(Spiceworks)

Problem: Segmentation of traffic is tied to network infrastructure; disconnected from business rules

Segmentation Chaos: Fragmentation

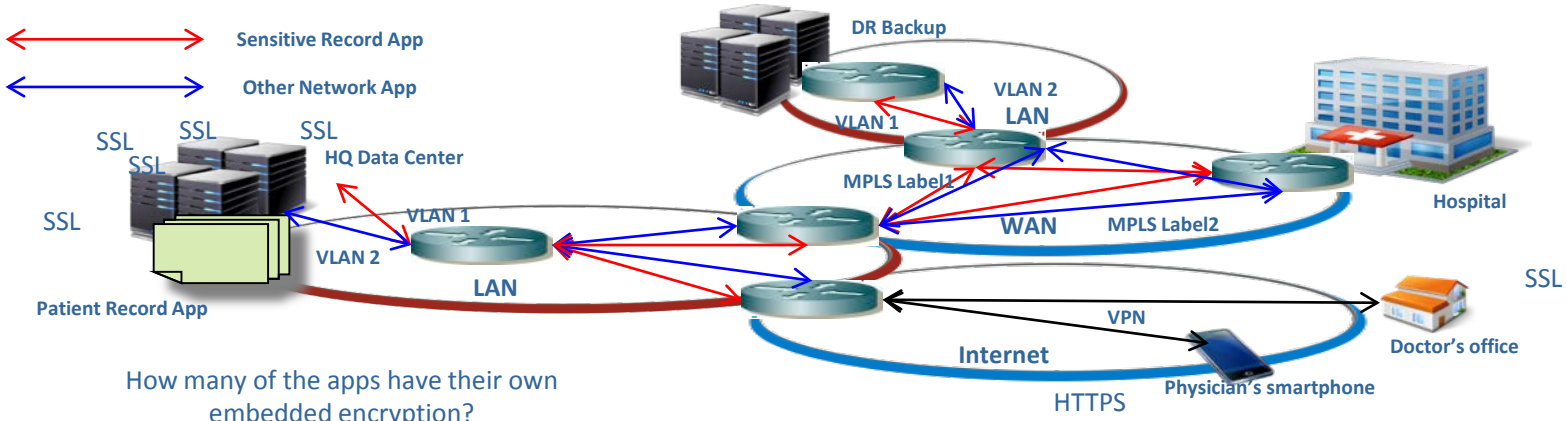
Attempting to isolate traffic hop by hop, app by app
Consumer grade encryption, out of your control
VLANs, ACLs, VPNs, IPsec, SSL, TLS, DMZs



Segmentation Chaos: Too Many Tools

Where are VLANs defined and enforced?
Are they encrypted?

How are WAN links encrypted?
Who controls keys?
How are they managed?



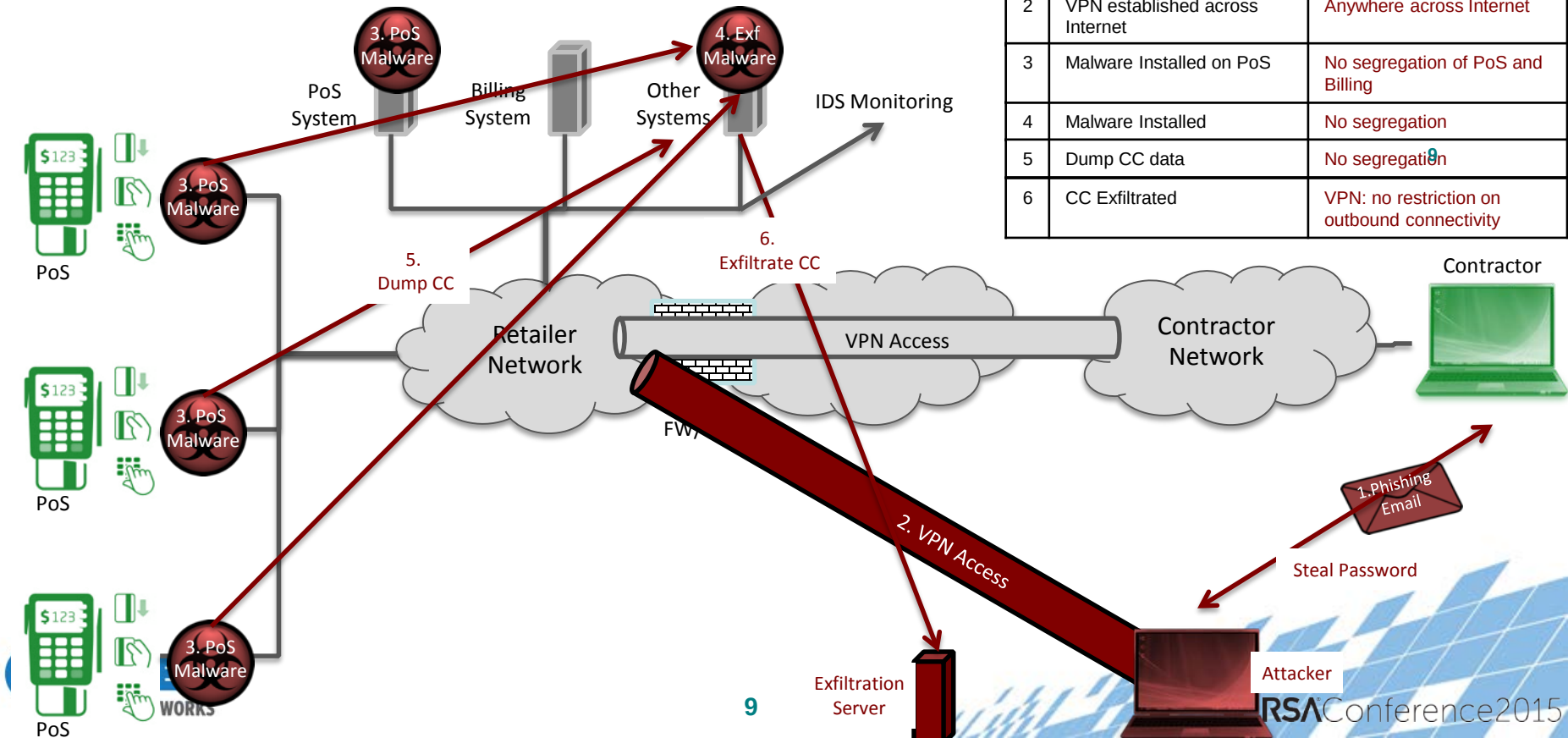
How many of the apps have their own embedded encryption?
Who controls it?
What's in it?
Do they contain Heartbleed?

Siloed
Fragmented
Gaps

How are apps encrypted to mobile devices?
Is it enterprise grade encryption?
Who controls keys and algorithms?

Epic Segmentation Fail

	Attack Steps	VPN: Protection Failed
1	Phishing Steals Password	Weak password security
2	VPN established across Internet	Anywhere across Internet
3	Malware Installed on PoS	No segregation of PoS and Billing
4	Malware Installed	No segregation
5	Dump CC data	No segregation
6	CC Exfiltrated	VPN: no restriction on outbound connectivity

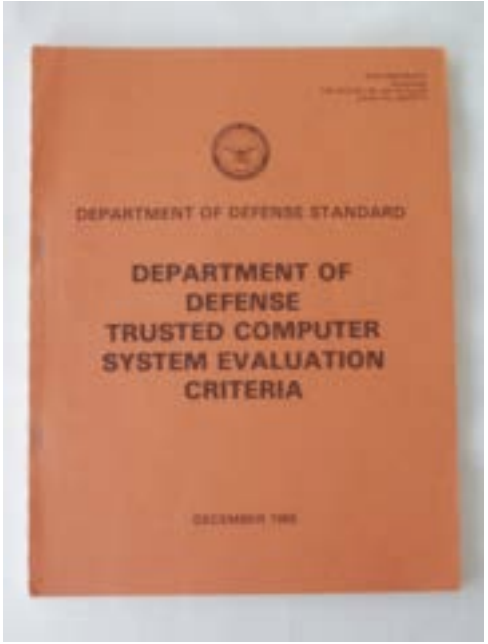


Back to the Drawing Board

What is Security? (Orange Book)

- Policy: Rules of Security
- Accountability: Identity and Authorization
- Assurance: Cannot be bypassed

Objective: Move IT security away from the infrastructure and closer to the business rules



A New Blueprint

What Is Crypto-Segmentation?

Role-based access to cryptographically isolated networked applications

- Crypto-segments defined per application based on business rules
- User roles and business policy determine access rights based on verified identity
- Maintain complete control of keys and key lifecycle
- Centralizes audit logging for all access
- Compromise of network, application, user does not compromise crypto-segments: no lateral movement

Crypto-Segmentation Architecture

Enterprise Directory

Users and Roles

Policy Orchestrator

Policies & Keys

App Crypto-Segments

CRM App

Billing App

Policy Enforcer

Policy Enforcer

Policy Enforcer

VPN

VPN

Sales

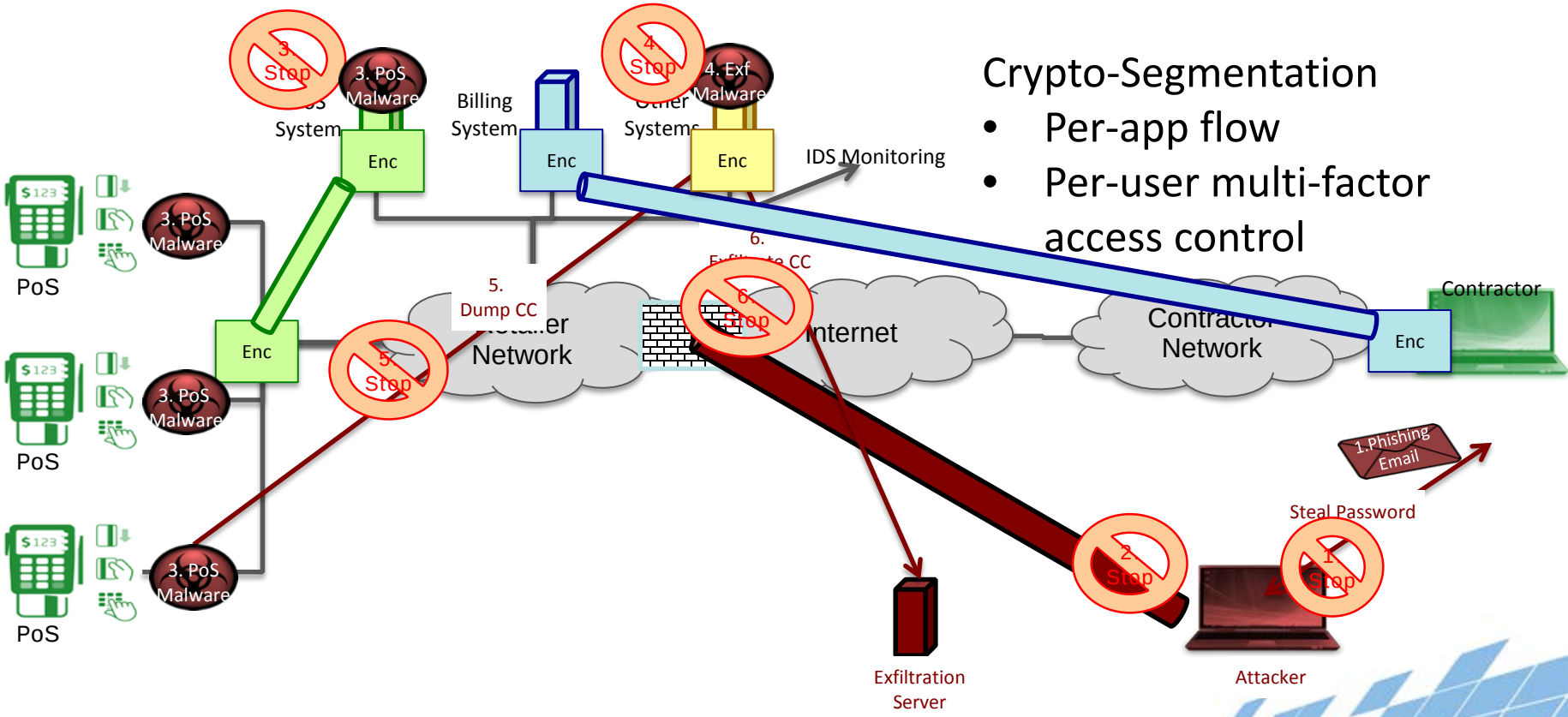
Admin

CERTES NETWORKS

Security Evolved

- Cryptographically assured segmentation
  - Compromises in one segment can not propagate to another segment
- Strong user identity and role enforcement
- End-to-end security with no network dependency
- Security team in control
  - Keys, policies, auditing: orchestrated across all apps, users, networks

Crypto-Segmentation in Action



Crypto-Segmentation

- Per-app flow
- Per-user multi-factor access control

Summary: Question the status quo

- What are your business-driven security requirements?
- What happens when they change?
- Does your current network security architecture help or hinder?
- How does it hold in the new realities of BYOD, mobile, public cloud, SaaS?
- What happens when a breach takes place?

Apply Crypto-Segmentation

- Make a list of your current applications
- Prioritize most sensitive
- Which user roles need access when and where?
- Crypto-segment along these dimensions
- Make Business needs drive security, not security risk drive business practices
  - I cannot secure this, it will not be on your mobile

RSAConference2015

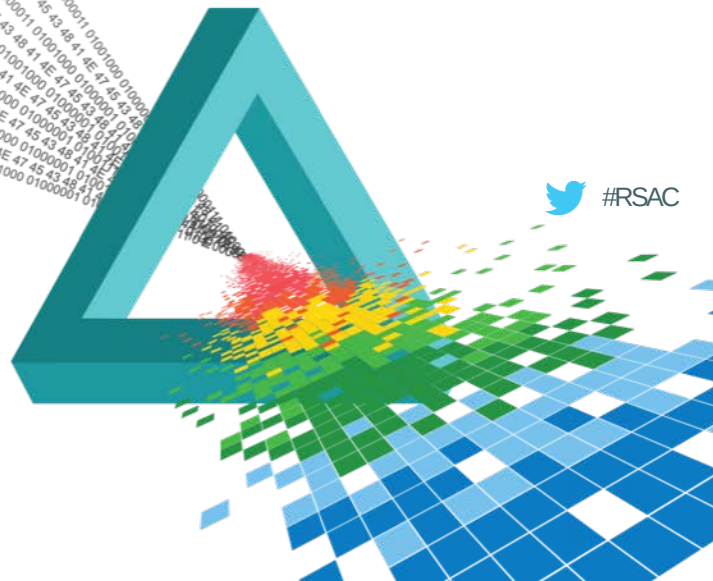
Singapore | 22-24 July | Marina Bay Sands

Thank you

Satyam Tyagi, CTO, satyam.tyagi@certesnetworks.com

Adam Boone, CMO, adam.boone@certesnetworks.com

CertesNetworks.com



#RSAC