Ending the information security arms race with end-to-end encryption

Presenting: STEALTH

by UNiSYS

Jill Walsh
October, 2013
Big Drivers for IT Security

Consumerization of IT

- Device explosion; app explosion
- Employee demands
- It’s no longer about “work/life balance” but “work/life integration”

Why not just plug in?

- Corporate due diligence
  - Standardized PCs
  - Standardized support model … based on PCs
  - Anti-virus/anti-malware and Patch Management
- Many infrastructures are Microsoft-centric

Proble...ple...bypass

Tablets don’t support this model

Problem 1 - Smartphones/tablets don’t support this model
Problem 2 – An increasing number of internet services bypass corporate security controls – on purpose

52% of employees paid for their work tablet
43% of employees use a home computer for work
38% of employees use unauthorized apps, software, or sites for work
35% of employees paid for their work smartphone

Source: A Unisys commissioned study conducted by Forrester Research, Inc., June 2012
Big Drivers for IT Security

Rise of the Advanced Persistent Threat (APT)

Operators have a full spectrum of techniques at their disposal

Conducted through continuous "low-and-slow" interaction to achieve objectives

Attacks are executed by coordinated human actions with capability and intent

Target  Foothold  Access  Deploy  Cover Up

Corporate Diamonds
Enterprise Administration (Active Directory)
Departmental infrastructure
Random spam
Spear phishing
Bad web site
Botnet C&C
Who are the Adversaries?
Card Processing Breach; ATM massive cyberattack

Hackers broke into internal computer network and card processing servers of financial companies and eliminated the withdrawal limits on prepaid debit cards.

The thieves distributed prepaid card numbers associated with hacked accounts to cashing crews around the world, which easily reprogrammed the account data on disposable gift cards.

Around the globe, thieves used these cards to withdraw $M from the compromised financial institutions.
Information Security Arms Race

Security Information and Event Management

- Intrusion Detection & Prevention
- Network Firewall & VPN
- Vulnerability Management
- Secure Remote Access
- Threat & Vulnerability Alerting
- Endpoint Security
- Application Security Services
- Network Security Services

Attacks Event Correlation Engine

Normalization of Element-specific log file data

- Unisys Monitored or Managed Security Elements
- Security Infrastructure, Network Devices, OS, database, & application logs

- Scanner: Asset Inventory & Vulnerability Scanning
- Assets & Vulnerabilities
- Threat Pattern Database
- Event Database

Portal: Unisys or Customer Ticketing System

Reporting: Incidents

Response & Remediation

Portal: Portal

Portal: Portal

Portal: Portal

Portal: Portal

Portal: Portal
Security Information and Event Management (SIEM)

• Getting more and more expensive – like big data
  – Software costs
  – Storage of all the log and traffic data/meta data
  – Processing
  – Network resources to move data from endpoint to SIEM

• At some level you have to have it …

For many companies, it’s a cost / risk juggle (CYF)

For advanced adversaries, traditional approaches aren’t working anyway
All Those Security Arms Race Technologies...

- What problems remain?
- Are they cohesively solving...
  - Asset segregation based on sensitivity of information?
  - Both internal and external threats?
  - Transmission security for Data in Motion?
  - Protection for End Points?
  - Operational requirements to detect, contain, respond and recover?

---

Washington Post Joins List of News Media Hacked by the Chinese

By NICOLE PERLROTH
Published: February 1, 2013

SAN FRANCISCO — The question is no longer who has been hacked. It’s who hasn’t?
Ending the Information Security Arms Race

- Identify important assets and who should have access
- Build a compartmentalized security model based on need-to-know
- Protect and enforce that security model with strong end-to-end encryption, properly managed keys and secured endpoints
Segmenting By Asset Sensitivity

- Segmenting the network virtually, into logical domains allows tighter security for defense-in-depth and compliance requirements.
- Segmenting by *user credentials* controls access to resources regardless if connection is from headquarters, a branch agency, or remote location.

*Enables security team to protect dynamically changing network infrastructure and services*
Enter Unisys Stealth™

A certified, scalable security innovation, uniquely positioned to protect mission critical network assets, incrementally and non-disruptively implemented, that makes data communication end points dark on a network.

Here’s what a hacker sees when Stealth is enabled.
Unisys Stealth Highlights

- Software driver running on endpoints
- FIPS 140-2 certified AES-256 cryptography
- Provides compartmentalized security via virtual communities of interest (COI) for predetermined endpoint users
- Authenticates and authorizes users based on identity, not network topology
- Executes low in the protocol stack – no effect on applications or existing networks
Stealth Enabling a Web Application
Application Environment Compartmentalization – one example

• Because Stealth is software, it can be deployed with
  – **no network changes** (no cabling, no VLAN or LAN changes, no new firewall rules)
  – **no application changes** – either code or configuration

• ... and if you chose to install only the data center components, there is
  – **no end-user impact** – or even awareness
Stealth Is Scalable, Consistent, End to End
And About Those Adversaries?
Card Processing Breach; ATM massive cyberattack

Stealth Solution:

- Logically compartmentalize existing financial institution network:
  - Cloak the Card Processing servers and applications from attackers and non-essential employees so systems are not accessible
  - Control system access from / to restricted web servers servicing the Internet and ATM transactions
- Card Processing Servers, applications and account data not compromised by intruders
Thank You

Merci