A School’s Blueprint to Secure Everything

Renault Ross CISSP, MCSE, CCNA, CHSS, CCSK, VCP5
US Information Security & Privacy Architect
Public Sector Strategic Programs
Agenda

- Key Trends & Snapshot of Today’s Threat Landscape
- Security Challenges in Securing Everything
- Recommendations and Strategies
Technology Trends

- **Data Growth**
- **Consumerization**
  - Mobile
  - Social
- **IT-ification**
- **Virtualization**
- **Cloud**
- **Threat Landscape**
Technology Trends

- **DATA GROWTH**
- **CONSUMERIZATION**
  - Mobile
  - Social
- **ITIFICATION**
- **VIRTUALIZATION**
- **CLOUD**
- **THREAT LANDSCAPE**
Technology Trends

- Data Growth
- Consumerization
  - Mobile
  - Social
- IT-ification
- Virtualization
- Cloud
- Threat Landscape

Key Trends
Internet of Things

Auto
- Telematics
- In-vehicle entertainment
- Navigation
- Safety services
- Concierge services
- Remote diagnostics
- Personalized insurance

Manufacturing
- Supply chain management
- Geo-fencing
- Machine diagnostics
- Inventory control
- Industrial automation control
- Equipment monitoring

Retail & Finance
- Smart payments, cards
- Point of sale terminals
- ATM
- Vending machine monitoring
- Digital signage and electronic billboards

Healthcare
- Home healthcare and hospital patient monitoring
- Remote telemedicine & physician consultation
- Body sensor monitoring

Utilities
- Meter reading
- Industrial controls
- Pro-active alerts
- Smart Grid applications
- Remote temperature control

Consumer Services
- Smart home appliances
- Connected home
- Video feed monitoring

Symantec
Threat Landscape
A fundamental shift...

Old Motivation
Hacking
Cyber Crime
Cyber Espionage
Cyber Warfare
What’s in common between Miss Teen and a Businessman?
THEY ARE BOTH TARGETED FOR ATTACK
THE SHOWBIZ COUNTDOWN

TODAY'S TOP SHOCKERS!
OUR #2: MISS TEEN USA SAYS SHE WAS HACKED, PRIVATE BEDROOM PHOTOS USED AS BLACKMAIL
DarkComet RAT Legacy disclaimer (EULA)

1. disclaimer of warranties and indemnity

1.1 phrozensoft.com makes no warranties, conditions, undertakings or representations of any kind, either express or implied, statutory or otherwise in relation to the software including without limitation any implied warranties or conditions of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement or arising from course of dealing, usage or trade. some states/jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you and you may have other legal rights that vary from state to state or by jurisdictions. without limitation to the foregoing, phrozensoft.com does not warrant that the software will meet your requirements or that the operation of the software will be error free or uninterrupted or that defects in the software will be corrected.

1.2 phrozensoft.com does not represent that you are entitled to remove any third party applications and disclaims liability for any recommendations made by phrozensoft.com, its employees and sub-contractors in connection with your use of the licensed product.

1.3 you shall fully and effectively indemnify phrozensoft.com for any claim, action, proceeding, liability or expense suffered by phrozensoft.com as a result of your use of the licensed product.

2. limitation of liability

2.1 you use the software at your own risk. to the maximum extent permitted by applicable law, in no event shall phrozensoft.com be liable to you or to those claiming through you for any direct, indirect, consequential, incidental or special damage or loss of any kind including, but not limited to, loss of profits, loss of contracts, business interruptions, loss of or corruption of information or data however caused and whether arising under contract or tort, including negligence, even if phrozensoft.com has been advised of the possibility of such damages.

2.2 if any limitation, exclusion, disclaimer or other provision contained in this licence agreement is held to be invalid for any reason by a court of competent jurisdiction and phrozensoft.com becomes liable thereby for loss or damage that may lawfully be limited, such liability whether in contract, tort or otherwise, will not exceed the fee paid by you for the software.
Targeted Attacks up 42% in 2012
Targeted Attacks by Industry

- Manufacturing moved to top position in 2012
- But all industries are targeted
Infection vectors

Spear Phishing
Send an email to a person of interest

Watering Hole Attack
Infect a website and lie in wait for them
The vulnerability being exploited is the browser and plugins:

- Plugins (flash, Acrobat, Silverlight, Skype...)
- Code (php, ActiveX, javascript, AS3)
- Browser
- Protocol (HTTP, HTTPS)
- Network (IP)
Threat Landscape

How are we being attacked?

• It can start with an attachment
• Buried inside may be an embedded ‘Flash’ object
• Which leverages a vulnerability to deliver malware
Threat Landscape

How are we being attacked?

- More likely it will be a link
- Seems innocuous, right?

- Well not so fast...
- Hover over the link to see the real link buried underneath
- Clicking the link brings you to a malicious web site
Threat Landscape

How are we being attacked?

• Or the web site itself will infect you just by visiting it...

• For example, the neighborhood pizza store might be infected

• How many pizza stores have a fulltime IT guy on staff looking out for trouble?
2010 Trends
Mobile Threats

“There’s an app for that...”
Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 MB of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1. Take your cash to one of this retail locations:
   - Walmart
   - CVS pharmacy
   - Walgreens

2. Get a MoneyPak and purchase it with cash at the register

3. Come back and enter your MoneyPak code to unlock your computer (5 attempts available)
Threat Landscape
Why is it hard to stop attacks?

1. Hacker develops threat

2. Hacker uses Tool to obfuscate executable

3. Tool generates clones that differ at the byte-level

4. Use cloud scanner to check for detection

5. Release undetected variants
The Internet of Things Is a Broad Area

* Adapted from Beecham Research
The Rising Number of “Things”

- Today, 7 billion people, 9 billion connected devices!
- By 2020, 50 billion “things” connected to the Internet

*From Cisco UBSG, April 2011*
Architecture Matters

Application logic, data and analytics can be placed anywhere

Local/Edge | Gateway | Cloud | Enterprise

Application | Data | Analytics
Trust / Governance

- When a device is contacted for the first time (a user, another device), is it trusted?
  - PKI as a root of trust
  - Employ reputation
  - Leverage a separate trusted channel

- Governance:
  - Policy definition, management, and enforcement
  - Compliance
Identity

- Billions of devices are going to be interconnected, so it is necessary to manage their identities in a scalable way.
- Eventually, each device will be addressable on the Internet to support end-to-end communication, so it requires a scalable way to discover a device’s address given its identity.
Fault Tolerance

- Devices may become faulty and stop working and even get compromised
- Many devices deployed in the field where there’s no management capability
- Fault tolerance:
  - Remote monitoring
  - Fault discovery by e.g., anomaly detection, intrusion detection, or remote diagnostics
  - Remote reboot, reprogramming, and software update
  - End-point protection by e.g., lock-down
Communications

- Heterogeneous communications:
  - Ethernet, dial-up, optics
  - WiFi, Cellular, ZigBee, Bluetooth, WiMax

- Different requirements for communication:
  - Low transmission latency for control networks
  - Small payload size, e.g., 8 bytes for CAN, and 128 bytes for ZigBee

- Secure communications channel:
  - Establish secure communication between devices/users using e.g., SSL-like handshake protocol
Security Recommendations In the Internet of Things

- **Develop and Enforce IT Policies**
  - Policy & standards modules, risk manager & vulnerability modules and solutions

- **Authenticate Device**
  - Two-factor authentication, Managed Public Key Infrastructure

- **Protect the information**
  - Loss Prevention, Encryption, Backup and High availability solutions

- **Manage the Infrastructure**
  - management, software delivery, assets, ticket management and mobile devices solutions

- **Protect the Infrastructure**
Governance Tools to Develop and Enforce IT Policy
Governance, Risk and Compliance

Audit Reports

Dashboards

External Policies

Standards

Entitlements

Questionnaires

Federated Data Processing and Analysis

CCS-Data Collection

3rd Party Data

ESM Manager
Authenticate Identities & Devices
Strong Authentication and MPKI

Public Key Infrastructure
- PKI service issues certificates for strong authentication, encryption and digital signing

VeriSign Identity Protection
- Shared cloud-based two-factor authentication solution offering multiple credential choices

Fraud Detection Service
- Risk-Based authentication and software-based fraud detection

Government

Endpoint

Application

Mobility
Protect the Information
Data Loss Prevention

Storage
- Data Loss Prevention
  - Network Discover
- Data Loss Prevention
  - Data Insight
- Data Loss Prevention
  - Network Protect

Endpoint
- Data Loss Prevention
  - Endpoint Discover
- Data Loss Prevention
  - Endpoint Prevent

Network
- Data Loss Prevention
  - Network Monitor
- Data Loss Prevention
  - Network Prevent
Encryption of sensitive data

Whole Disk

Removal Hard-drive

Help Desk
Manage the Infrastructure
Enterprise Systems Management

- Systems Management Platform
- SECURITY
- INFORMATION RISK & COMPLIANCE
- STORAGE
- INFRASTRUCTURE OPERATIONS
- BUSINESS CONTINUITY

- Dell Management Console
- Dell Client Manager
- vPro™ enabled computer management
- HP Client Manager

- Mobile Security Management
- Backup Management
- Application Virtualization
- Power Management
- HelpDesk Management
- Patch and System Management

Third-Party Solutions
Protect the Infrastructure
Threat management solutions

Endpoint
- Block Viruses, Malware, and Spyware
- Enforce Compliance
- Recover Desktops

Messaging
- Secure Mail Servers
- Block Spam at the Gateway
- Prevent Data Loss

Web
- Stop Web Attacks at the Gateway
- Control Web Applications
- Detect Compromised Endpoints

Logo: Symantec
Summary

- Network monitoring
- Anomaly detection and reporting
- Information and event management from all network and host sources
- Data management
- Intrusion protection / detection
- Resource lockdown

Operational Security
- CSP
- Inventory & Asset Mgmt

Information Protection
- Data Loss Prevention
- Encryption

Embedded Security
- SEP
- mPKI
- CSP

Manage Data
- Storage Foundation
- NetBackup
- Network Heuristics

Devices
- Operational Security
- Information Protection
- Embedded Security
- Manage Data

Information and Event Management from all network and host sources.
- Data management
- Intrusion protection / detection
- Resource lockdown
- Encrypt information
- Authenticate devices
- Managed / hosted PKI & device level certificates
- Controlling and securing systems
- Intrusion protection / detection
- Resource lockdown
- Application whitelisting

Network Monitoring
- Network monitoring
- Anomaly detection and reporting
- Information and event management from all network and host sources
- Data management
- Intrusion protection / detection
- Resource lockdown

Symantec Security in IoT

Network Heuristics

Data Loss Prevention

Encryption

CSP

Inventory & Asset Mgmt

Data Management

Intrusion Protection

Resource Lockdown

Application Whitelisting
Thank you!

Renault Ross
Renault_Ross@symantec.com