CYBER SECURITY:

BEST PRACTICES FOR INTERNATIONAL BUSINESS

Dr. Raimund K. Ege
NIU - Computer Science
ege@niu.edu

Overview of Presentation

- Assessment of the current
  threat landscape and attack modes
- Best Practices to protect your
  business, property and customers
- Future of
  cyber threats and security measures

Current Threat Landscape

- Comparisons indicate that:
  - Average bank robbery amounts to $2,500
  - Average bank fraud amounts to $25,000
  - Average computer crime amounts to $500,000
- Current Cybercrime estimate:

  $100bn to $3trn
- But:
  - Large aspects of business are conducted online
  - Opt-out is not an option

Example: Target

- Exposed credit card and personal data on more than 40, 70, 110 million consumers
- POS malware collected credit card data

- 2 questions:
  - How did the malware get in ?
  - How did the “loot” get out ?

Example: Target

- Accessed Target system via stolen credentials
  - Outside vendor: HVAC contractor
  - Infected via email: Citadel malware
  - free version of Malwarebytes Anti-Malware
- Access limited to electronic billing, contract submission and project management
- Access via portal: privilege escalation via Active Directory

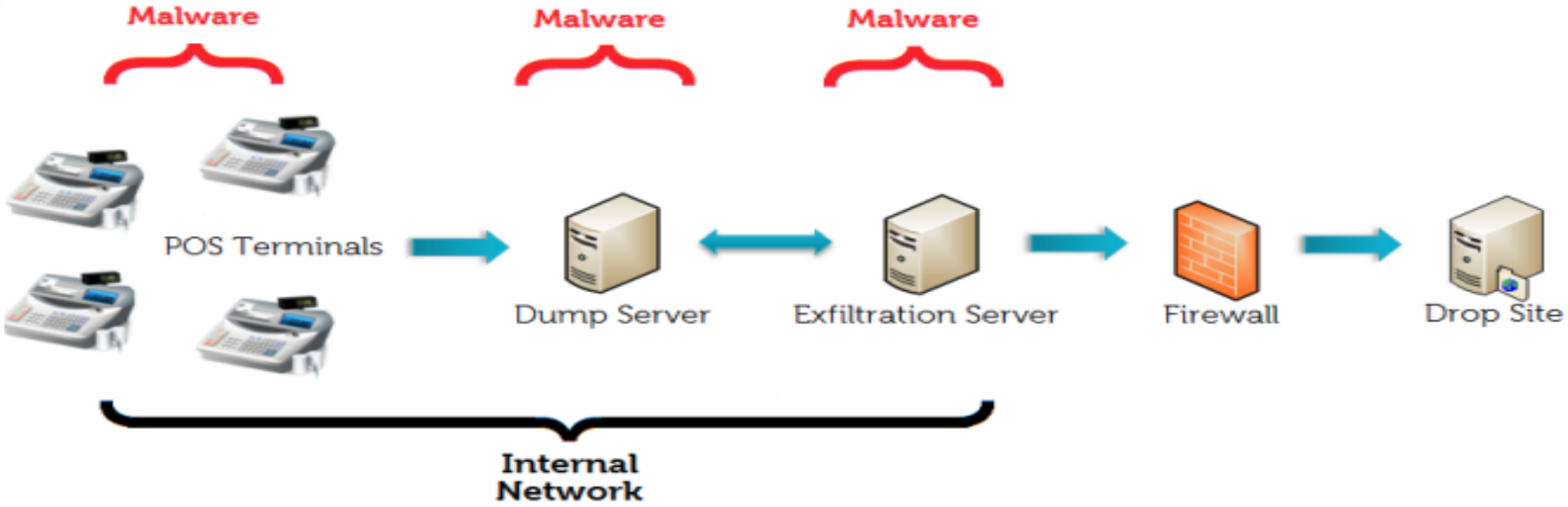
Example: Target

- Reconnaissance:
  - Target's Supplier Portal: includes wealth of information for vendors/suppliers about how to interact with the company, submit invoices, etc.

Example: MS Excel file, with meta data

reveals: user name, internal host name

Example: Target



The Problem with Credit Cards

- US uses swipe and sign
- Any world traveler knows:

  Chip and PIN

- Why US behind ?
  - US is largest market: in the past fraud elsewhere
  - Cost of infrastructure upgrade

Next Steps for Credit Cards

- Non-US: adopted EMV system
  - Chip and PIN
- Half of credit card fraud now occurs in US
- US migration
  - Chip and signature
  - Chip and PIN
- BUT: online transactions ?

Example: Apple iOS

- Technical detail: programming error in key routine of SSL handshake algorithm
  - Skips verification of server certificate
- Allows “man-in-the-middle” attack

- Scenario: intercept and decrypt the private contents of a supposedly secure connection

Example: NSA vs. RSA

- RSA algorithm key to security protocols
- RSA had consulting contract with NSA

- US corporation provide Internet infrastructure components:
  - Microsoft, Google, Cisco, …

- Ex.: Huawei telecom equipment maker

Key to Success: Vulnerability

- a system susceptibility or flaw
- attacker access to the flaw
- attacker capability to exploit the flaw

- Software/system
  - Bug or feature
- Network
  - Protection, architecture
- Devices
  - BYOD
- Access control: credentials
  - Management, escalation
- Organizational
  - Policies, plans & procedures

Anatomy of a Modern Attack

ADVANCED TARGETED ATTACK

- Reconnaissance: phishing
- Select vulnerabilities
- Delivery: infiltration
- Reconnaissance: lateral move
- Command & Control
- Apply payload
- Exfiltration
- Maintenance

What the Future holds

- Concept: Arms Race

- Future of cyber threats
  - expect zero-day vulnerabilities
  - arms bazaar of zero day vulnerabilities

- Security measures that are being developed
  - Education: increase awareness and sensitivity

Arms Race

- Should you be afraid of new technology
  - Lesser used, lesser exploited

- Example: MacOS
  - SSL breach
- Example: Cloud computing
  - Secured along host/topology lines
  - New factor: load balancing
    - Dynamic change of topology

Outlook: Attack Vectors

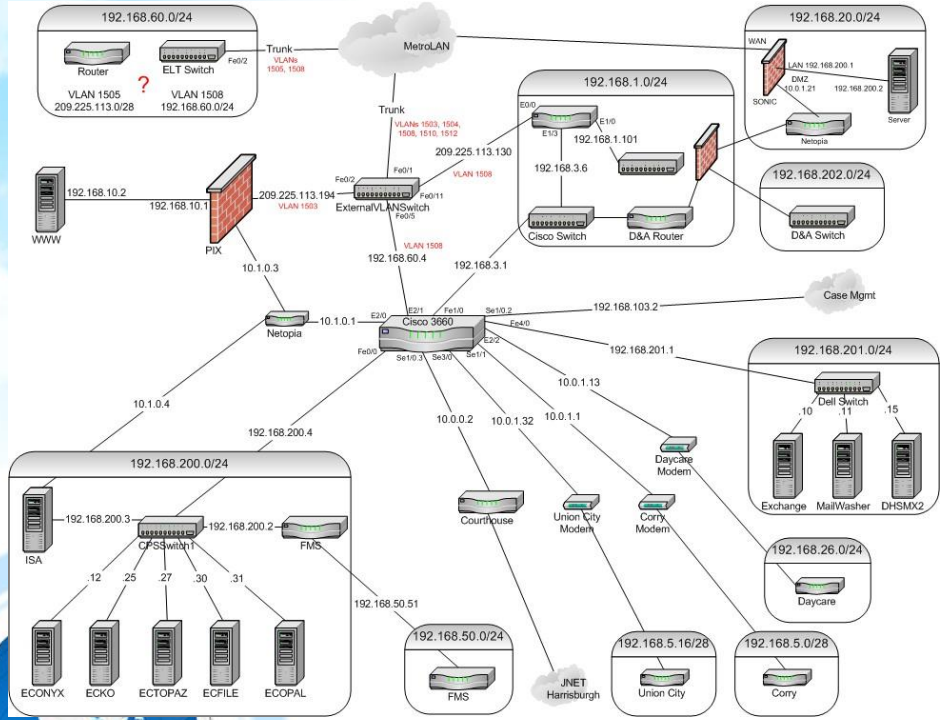
- Targeted attack types
  - Multiple & escalating path segments
- Exploit aging software/system
  - Java 6, Windows XP
- Internet of Everything: IoE
- Arms bazaar of vulnerabilities
- Botnets: Infrastructure for criminal community
- Deep web

Now, let’s concentrate on

Best Practices for Companies

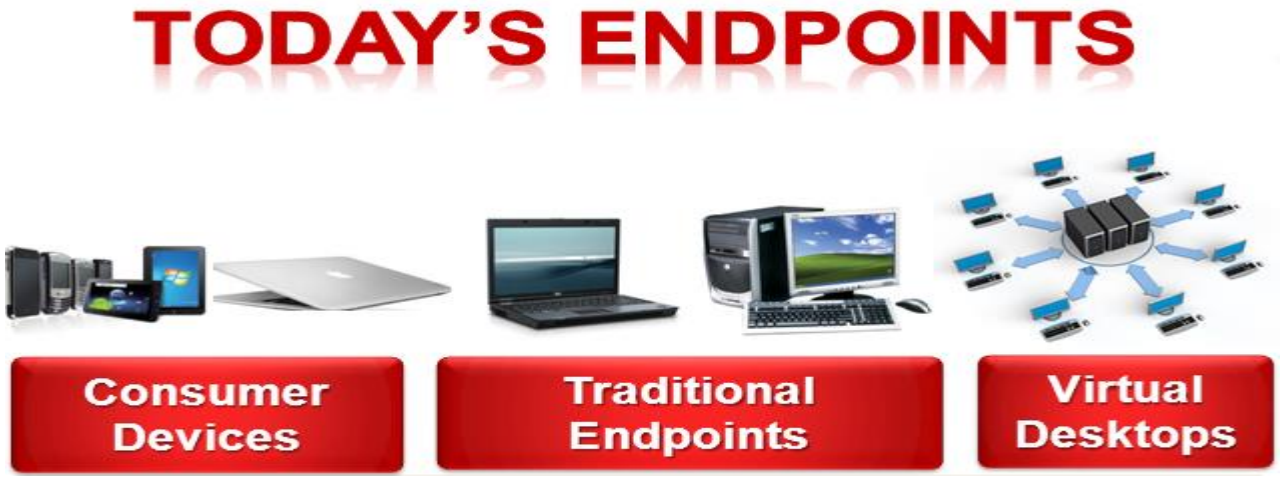
- Know your assets
  - Business critical data
    - Intellectual property, operational data
    - Customer data, communications
  - Business critical services
  - Your reputation

Best Practices: know your network



- Node location(s), cloud
- OS, platform systems
- Network
  - Topology/segmentation
  - Access points ?
- Encrypt: data & links
  - Maintain your keys

Access to Business Critical Data



Secure BYOD

Manage the Devices

- Device Discovery
- Device Enrollment
- Device Provisioning
- Asset Tracking
- S/W Management
- Remote Control

Protect the Data

- Encryption
- Remote Wipe
- Remote Lock
- SIM Change/ Watch
- Feature Lock
- Password Policy

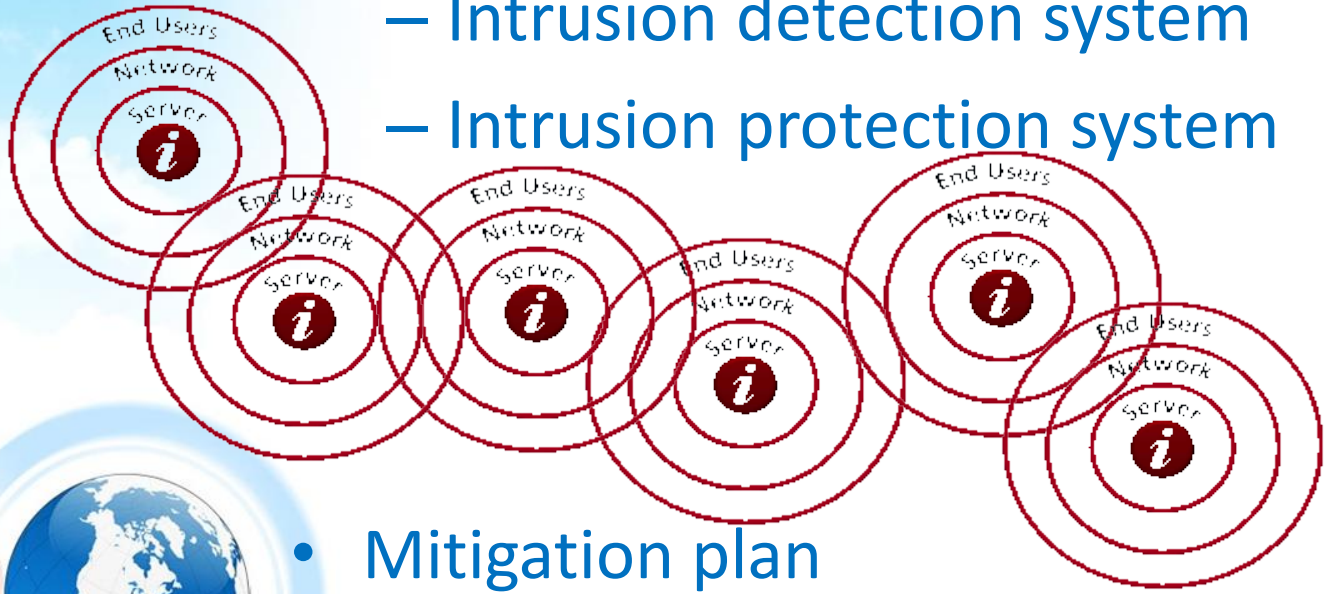
Secure the Devices

- Anti-Malware
- Firewall
- Web Threat Protection
- Email Security
- Call/ SMS Anti-Spam
- App Control/Lock-down

Central & Policy Management

Best Practices: monitor

- Monitor your assets
  - Intrusion detection system
  - Intrusion protection system



- Mitigation plan

Best Practices when Traveling Abroad

- Protect your information, communications and the devices you transmit information on
- Visit the State Department's website prior to visiting a country to update yourself on safety information
- Leave non-essential electronics at home: safe

Best Practices when Traveling Abroad

- Before you go – if you take it, protect it
  - Back up your electronic files
  - Remove sensitive data
  - Install strong passwords
  - Ensure antivirus software is up-to-date
  - Separate work from play

Best Practices when Traveling Abroad

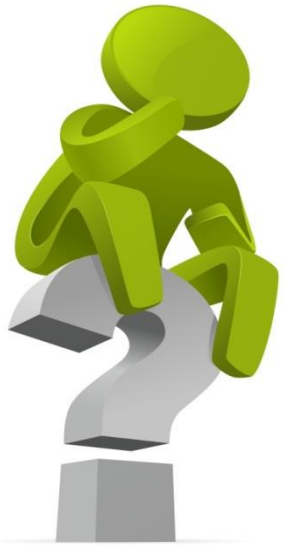
- While traveling
  - Don’t assume your information is safe – thieves can be invisible
  - Keep your eyes on your electronics
  - Smartphones may connect to local networks abroad: turn off PAN
  - Don’t use the same passwords or PINs abroad that you do in the U.S.

Summary of Presentation

- Assessment of the current threat landscape and attack modes
- Best Practices that enterprises use to protect their business, property and customers
- Future of cyber threats and the security measures that are being developed

Comments & Questions

International Cyber Security



Dr. Raimund K. Ege
ege@niu.edu