Securing ACH and Wires Transactions & the Challenge Manager Token Service

Liam Yu, Senior Product Manager & Jason Duke, Business Analyst
November 19, 2009
Agenda

• Threat Landscape - What customers are facing
• How Digital Insight can help
• The Challenge Manager Token Service and how it protects your commercial customers
• Corporate Banking Security Best Practices
The Threat Landscape & How Digital Insight Can Help
Online Fraud at an All Time High Nationwide

• Industry Online Crime up Nearly 600%
  • DI Security fraud data shows dramatic increase
  • Increase is specifically with fraudulent ACH and Wire payments
  • Targeting small business and smaller FIs

• Accelerated fraud drives increase warnings to Banks
  • FS-ISAC – 9/30/09
  • FDIC – 9/26/09
  • NCUA – 9/25/09

• Increased confusion & anxiety in the public

• Need for increased awareness in business segment
New Threats are Creating Greater Concerns

• **New Trend:** cybercriminals use a combination of Trojans and money mules to successfully avoid anti-fraud

• **New Crimeware/Stealware Trojans** - URLZone, ZeuS, Clampi
  – Focus on executing fraudulent ACH/Wires–not just password stealing

• **New Hacker Toolkits:**
  – Only costs $100-$300
  – Inserts exploiting code to vulnerable websites (legitimate or fakes)
    • Facebook, MySpace, YouTube, LinkedIn, Hulu & other sites with image and video
  – Once a visitor visits one of the infected websites, an exploit code installs a Trojan on the PC in use.
  – Examples of targeted applications exploits
    • Audio and Video (e.g. Adobe Flash – Vulnerability July 23, 2009, security advisory APSA09-03)
Anatomy of the New Crimeware

• **New Trojans such as URLZone, ZeuS, Clampi:**
  – Logs credentials and activities of bank accounts
  – Takes screenshots of webpages served by the websites
  – In some cases Trojan will present false forms on Bank websites that look accurate to users
  – Rewrites the account and payment instructions sent to processor thus stealing money from the compromised accounts w/o user knowledge
  – It hides its fraudulent transaction(s) in the report screen of the compromised account
  – Trojan servers send instructions over HTTP about the amount to be stolen and where the stolen money should be deposited
  – It also logs and reports on other web accounts (e.g., Facebook, PayPal, Gmail) and banks from other countries
How the Attack Works

Injects its own data collection forms onto legitimate HTML site or simply rewrites the ACH/wire details to send to backend processors.

1. Trojan wakes up & invades browser
2. Injects its own instructions
3. Sends false account # & $ amounts
4. Uses token authentication
Again: The use of tokens is an essential layer of security. The Layered Approach involves several layers of security:

1. **Original Site**
2. **Fraudulent ACH/Wire**
3. **Wire/ACH Creator**
   - BUT CANNOT APPROVE
4. **SecurID Token Approver only**
5. **Reveals False Account # & $ Amounts**
6. **Token Authentication**
   - Processor
7. **Separation of Duties Control**

These layers work together to prevent unauthorized access and reduce the risk of fraud.
Layered Protection can Mitigate Threats

Fundamentals for your Customers

- Keep antivirus protection up-to-date
- Keep OS, Browser, email patches up-to-date
- Keep video/media applications up-to-date
- Use network & desktop firewalls
- Be aware of phishing attacks
- Do not use business machine to surf social sites (e.g. Facebook)
The Challenge Manager Token Service: How it Protects your Commercial Customers
Challenge Manager – What is it?

• Challenge Manager is a service within the Corporate Banking Application where the bank can establish and administer challenge points within the system

• Challenge points may be placed on any service invocation including login

• Challenges can be set for any and all users in the system and can be set at the customer and user level

• Challenges can be set to occur once per session or every time a user clicks on a service

• Challenge Manager works with RSA’s SecurID Server to provide a fully FFIEC compliant MFA solution
Challenge Manager – How Does it Protect?

• Two-factor authentication: something you know (IDs & Passwords) and something you must have (token)

• The token contains a clock and a unique seed number, coupled with an unique algorithm, produces a new Token Code every 60 seconds

• Each deployed token is registered to a user and synchronized with RSA’s SecurID server

• Corporate Banking validates the Token Code entered using the synched clock, seed number and the same algorithm

• User entered Token Code = Server calculated Token Code = User authenticated
Challenge Manager and SecurID – Adding to the Armor

**Authentication**
- Login
  - Cust Code
  - Cust Password
  - User Code
  - User Password
  - DI Challenge or Passmark

**Access**
- Set by User Administration
  - Services
  - Accounts
  - Functions
  - Limits

**Authority**
- Payment Initiation
  - Service
  - Account
  - User Limit
  - Transaction Limit

---

**Authentication**
- Login
  - Cust Code
  - Cust Password
  - User Code
  - User Password
  - DI Challenge or Passmark

**Access**
- Set by User Administration
  - Services
  - Accounts
  - Functions
  - Limits

**Authority**
- Payment Approval
  - Service
  - Account
  - User Limit
  - Transaction Limit
  - Company Limit
Best Practice # 1 – Separation of Duties

Separation of Duties
Prevents one single FI employee to have access to the entire end user credentials
Best Practice # 2 – Password Complexity

- Increase Length
- Add Complexity
- Password Pattern
- Password Lockout
Best Practice # 3 – Dual Administration

Dual Administration Control
One person updates and another person approves
Best Practice # 4 – Dual Transaction Approval

Dual Transaction Control
One person initiates and another person approves
Additional Actions

• Establish policies for only specialized and trained officers to sell and implement wire/ACH origination services

• Educate customers on risk management and fraud prevention controls and practices

• Set strong control criteria as (policy) defaults

• Require additional signatory acknowledgement if default strong control is declined

Example:

_______ By signing here, authorized officer of xxxxxxxx decline the use of the recommended security control settings.
**Additional Actions**

- Encourage customer Admin/Owner to run Activity Reporting daily.

- Promote the use of resetting Company Password on an “irregular” basis – to rid of unsanctioned users unannounced

- Utilize Balance Alerts beyond nice-to-know information, think fraud protection and prevention

- Limits, limits, limits
  - Company
  - User
  - Transaction
Thank you
References

• Online Crime up Nearly 600% in '09
  - http://www.fraudwatchinternational.com/phishing/
• FDIC Alert
• FS-ISAC
• NCUA
• Bank suits for lack of security online controls
• Adobe Vulnerability
  - http://www.us-cert.gov/cas/techalerts/TA09-204A.html