Cash is King
Who’s Wearing Your Crown?
Accounting Systems Fraud in the Digital Age

Tom Eston and Brett Kimmell
Agenda

• Introduction to Accounting Fraud
• Microsoft Dynamics Great Plains
  – Vulnerabilities and Attack Vectors
• Attacking the Users of Dynamics GP
• Fraud with Custom Malware (Mayhem)
• The Attacks: How to Commit Fraud
• Accounting Controls to Prevent Fraud
• Conclusions
About Your Presenters
Tom Eston

• Manager of the SecureState Profiling & Penetration Team
• OWASP Contributor
  – Mobile Threat Modeling Project Lead
  – OWASP Testing Guide v4
• SANS Mentor
• Security Blogger/Researcher: Spylogic.net
• Podcast Co-host: Social Media Security Podcast
• Speaker: Black Hat USA, DEFCON, ShmooCon, DerbyCon, SANS, MSI, OWASP AppSec
Brett Kimmell

• Manager of the Risk Management Practice at SecureState
• CISSP, CISA, CISM, CPA, CITP, PCI QSA
• Previously the Director of Information Systems and CFO for United Way of Summit County
Introduction to Accounting Fraud
When We Break In

• Penetration Testers and Attackers do this every day!
• Low hanging fruit (Apache Tomcat, JBoss, MS08-067)
• Easy to evade technical security controls
• Find the most sensitive data
  – Passwords, SSNs, PCI data, PHI, Proprietary
• Screenshot, Report, Profit, Repeat
• Nothing new here...
Photo Credit: http://cosine-security.blogspot.com/2011/10/derbycon-retrospective.html
What If?

• We could demonstrate *real* business risk?
• Typically this is financial risk and hits the bottom line of an organization
• Attack the accounting and financial systems
• We could test the non-technical accounting controls (not like an “audit”)
Technical Controls 101

- Confidentiality
- Integrity
- Availability

Technical controls can only go so far. When they fail (and they will) what do you rely on?
Accounting Controls 101

- Accuracy
- Timeliness
- Relevancy
- Reliability
- Consistency
- Comparability
The Problem?

• Accounting controls may not be in place
  – Or properly implemented
• Limited resources
• Limited skill set
• Limited time

It’s very unlikely that accounting departments are reconciling every account each month!
Traditional Accounting Fraud

• Insider Embezzlement
• Overstating Profits
• External Check Fraud
• Insider Fraud
  – Kickback schemes, skimming, sales fraud, etc.

Primary Control: Reconciling Bank Accounts!
Accounting Fraud Examples

Akron woman accused of stealing more than $1.78 million from her boss

Published: Thursday, July 30, 2009, 3:30 PM    Updated: Thursday, July 30, 2009, 4:11 PM

By Michael Sangiacomo, The Plain Dealer

AKRON, Ohio — A 43-year-old executive assistant at a development company stole more than $1.78 million from her boss’ checking account over eight years, police said.

Karin Goeldi was charged with aggravated theft. She worked for Cedarwood Companies. Police declined to identify the boss for honoring his request for anonymity.

"She was given access to her boss' personal checking account, and she was able to write checks on it," said police spokesman Lt. John Burke.

"From 2001 until July 13, she repeatedly wrote checks on that account and turned them over to cash. The amount taken is more than $1,780,000."

The Dalton Police Department is asking for the public's help with identifying a man who used a counterfeit check to purchase more than $3,300 worth of merchandise from Lowe's on Cleveland Highway in Dalton and then had the merchandise refunded for gift cards.

The incident happened on Sept. 4, and was reported to police later in the month after the victim discovered a bad check had been written on his account for $3,360. Upon investigating with his bank, the victim discovered that a check had been counterfeited with his account number and made to appear to be a business check. The address on the check was the same street as the victim's, but the wrong number.
Microsoft Dynamics Great Plains
Microsoft Dynamics GP

- One of the most popular accounting systems in the world for medium to large size businesses
- Microsoft purchased GP from Great Plains Software for $1.1 Billion in 2000
- Written in Dexterity specifically for GP
- As of 2010: 41,000 companies use GP
Microsoft Dynamics GP - Users

• No Windows Authentication (Active Directory) integration available (out of the box)
  – User accounts are created, managed and stored by SQL Server
• SQL Server “SA” account is the most powerful
• DYNSA owns all the GP databases. Performs privileged actions without the SA account in GP.
• Regular user accounts perform daily actions
Microsoft Dynamics GP

- Uses “client-server” architecture
- Application runs on the client, not the server
Locating the GP Systems and Database
System Naming Conventions

• Conduct DNS or NETBIOS queries
• Network shares with GP client installation
• Typical names we’ve found on networks:
  – GP
  – GP-PORTAL
  – DYNAMICS
  – DYNAMICS_DB
  – GREAT PLAINS
  – ACCOUNTING
  – FINANCE
Additional Recon

• Most Critical: GP SQL Server
• Others systems include:
  – The GP client applications (user workstations)
  – GP Business Portal (SharePoint)
• Company Intranet
  – Usually reveals GP and/or accounting system documentation
• Network Shares
  – Sometimes the GP application is shared on the SQL server!
Attack Vectors in GP
Vulnerabilities in GP

• DoS and remote overflow vulnerabilities in GP version 9 and lower

• Weak cipher for the system password (2010)
  – Debunked by Microsoft as a real issue

• Typical SQL Server vulnerabilities and misconfigurations
  – Example: Local Administrator group added to the “sysadmin” role on the SQL Server
Attacks We Like for Fraud

• Gain access to the GP SQL database directly
• GP user account hijack from the client
• Process injection via custom malware on the client
Attacking the Database

- Goal: Modify and create GP database entries to commit fraud
- Easy with direct access to the SQL server
- One problem...
- How do we know what to modify to commit the fraud?
GP Table Naming Conventions

- GP Tables are not named with good descriptions...
- There is good news though!
# GP Table Prefix Identification

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Module</th>
<th>Prefix</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>GL</td>
<td>General Ledger</td>
<td>AA</td>
<td>Analytical Accounting</td>
</tr>
<tr>
<td>AF</td>
<td>Advanced Financial Analysis</td>
<td>DTA</td>
<td>Multi-dimensional Analysis</td>
</tr>
<tr>
<td>PM</td>
<td>Payables Management</td>
<td>SY</td>
<td>System or Company</td>
</tr>
<tr>
<td>RM</td>
<td>Receivables Management</td>
<td>AHR</td>
<td>Advanced HR</td>
</tr>
<tr>
<td>SOP</td>
<td>Sales Order Processing</td>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>POP</td>
<td>Purchase Order Processing</td>
<td>BM</td>
<td>Bill of Materials</td>
</tr>
<tr>
<td>IV</td>
<td>Inventory</td>
<td>DD</td>
<td>Direct Deposit</td>
</tr>
<tr>
<td>IVC</td>
<td>Invoicing (NOT SOP)</td>
<td>EXT</td>
<td>Extender</td>
</tr>
<tr>
<td>UPR</td>
<td>US Payroll</td>
<td>MC</td>
<td>Multicurrency</td>
</tr>
<tr>
<td>CM</td>
<td>Cash Management (Bank Rec)</td>
<td>SVC</td>
<td>Field Service</td>
</tr>
<tr>
<td>LK</td>
<td>Linked Transactions</td>
<td>ASI</td>
<td>SmartList Favorites</td>
</tr>
<tr>
<td>ME</td>
<td>EFT</td>
<td>ERB</td>
<td>Excel Report Builder</td>
</tr>
<tr>
<td>PA</td>
<td>Project Accounting</td>
<td>EXT</td>
<td>Extender</td>
</tr>
<tr>
<td>FA</td>
<td>Fixed Assets</td>
<td>SLB</td>
<td>SmartList Builder</td>
</tr>
<tr>
<td>PDK</td>
<td>Personal Data Keeper</td>
<td>CPY</td>
<td>Canadian Payroll</td>
</tr>
</tbody>
</table>

Credit: Leslie Vail

http://dynamicsconfessions.blogspot.com/2012/05/data-flow-and-table-names.html
**GP Table Identifiers**

<table>
<thead>
<tr>
<th>Table Number</th>
<th>Table Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Master Tables</td>
</tr>
<tr>
<td>10000</td>
<td>Work Tables</td>
</tr>
<tr>
<td>20000</td>
<td>Open Tables</td>
</tr>
<tr>
<td>30000</td>
<td>History Tables</td>
</tr>
<tr>
<td>40000</td>
<td>Setup Tables</td>
</tr>
<tr>
<td>50000</td>
<td>Temp Tables</td>
</tr>
<tr>
<td>60000</td>
<td>Relation Tables</td>
</tr>
<tr>
<td>70000</td>
<td>Report Options Tables</td>
</tr>
<tr>
<td>80000</td>
<td>Posting Journal Reprint Tables</td>
</tr>
<tr>
<td>90000</td>
<td>Mixed bag – no standard type</td>
</tr>
</tbody>
</table>

- Put the prefix with the identifier to determine the table function
- PM10000 = Payables Management Work Table
Attacking the GP User
Who to Target?

- Accounting Department Users
- Controller
- Bookkeeper
- CFO
- The Accountant
The Goal

• Compromise the user’s workstation
  – GP application is installed there!
• GP login and password
• Compromise other workstations, pivot to the accounting users
• Create backdoor into the user’s workstation(s)
Example Scenario

• Harvest accounting department usernames and emails via LinkedIn
• Create targeted phishing email
• Link to download malicious attachment
  – “Click here to install the latest GP patch!”
• Mayhem ensues...or installs (more on this in a minute)
Creating the Perfect Fraud via Custom Malware
Who Wants to Create Mayhem!

• Who’s seen the “Office Space” Movie?
• Considered a “cult classic” from a Hollywood perspective
• Install virus (via floppy disk), infect accounting system, shave off a fraction of a penny of each transaction, check account balance, profit!
FILE COPY IN PROGRESS....
$ PROFIT $
Introducing: Mayhem Malware

- Proof of Concept code created by Spencer McIntyre of the SecureState Research & Innovation Team
How Mayhem Works

• Uses function hooking and library injection to execute within the context of the GP frontend
• Goal: Open a channel back to the attacker so commands can be made via the GP frontend
• Mayhem is injected at runtime and can use patching techniques
How Mayhem Works

• Mayhem creates hooks in key locations
  – Most important: calls to ODBC32 library
• Mayhem monitors this and then allows injection of SQL commands into the database as the authenticated user
• A HTTP backdoor is created which allows on the fly modification of SQL commands by the attacker
• More details on Mayhem in our whitepaper
The Attacks:
How Fraud Can be Committed
Manipulating Existing Vendor Records’ Remit-To Address
Manipulating Existing Vendor Records’ Remit-To Address

<table>
<thead>
<tr>
<th>VENDORID</th>
<th>VENDNAME</th>
<th>VNDCHKNM</th>
<th>VENDSHNM</th>
<th>VADDCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A Travel Company</td>
<td>A Travel</td>
<td>A Travel</td>
<td>PRIMA</td>
</tr>
<tr>
<td>2</td>
<td>Advanced Office Systems</td>
<td>Advanced Office Systems</td>
<td>Advanced Office</td>
<td>PRIMA</td>
</tr>
<tr>
<td>4</td>
<td>AmericaCharge</td>
<td>AmericaCharge</td>
<td>AmericaCharge</td>
<td>PRIMA</td>
</tr>
<tr>
<td>5</td>
<td>Attractive Telephone Co.</td>
<td>Attractive Telephone Co.</td>
<td>Attractive</td>
<td>PRIMA</td>
</tr>
<tr>
<td>6</td>
<td>Associated Insurance Inc.</td>
<td>Associated Insurance Inc.</td>
<td>Associated Insu</td>
<td>PRIMA</td>
</tr>
<tr>
<td>7</td>
<td>Australia</td>
<td>Australia</td>
<td>Australia</td>
<td>AUSTRALIA</td>
</tr>
<tr>
<td>8</td>
<td>Beaumont Construction</td>
<td>Your Company Name Here!!</td>
<td>Beaumont Constr</td>
<td>PRIMA</td>
</tr>
<tr>
<td>9</td>
<td>Bergeron Communications Sol.</td>
<td>Bergeron Communications Sol.</td>
<td>Bergeron Commun</td>
<td>PRIMA</td>
</tr>
</tbody>
</table>

Query executed successfully.
Manipulating Existing Vendor Records’ Remit-To Address
Remit-To cont......
Remit-To cont......
Create a New Vendor and Manual Check Entry (Mayhem PoC)
Increase Customer Credit Limit
Increase Customer Credit Limit

CREDTLMT (Credit Limit) in PM00200: (Thanks to Bud Cool, a frequent contributor to the Microsoft GP Newsgroup, for this information!) 0 – No Credit, 1 – Unlimited, 2 – Amount. Note: If CREDTLMT = 2 then CRLMTDLR contains the amount of the credit limit, otherwise CRLMTDLR is zero.
Credit Balance in Customer Account, Get a Refund

<table>
<thead>
<tr>
<th>General Ledger Distributions</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Number</td>
<td>Account Description</td>
<td>Account Type</td>
<td>Debit Amount</td>
<td>Credit Amount</td>
<td></td>
<td></td>
</tr>
<tr>
<td>000-1100-00</td>
<td>Cash - Operating Account</td>
<td>CASH</td>
<td>77,777.77</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>000-1200-00</td>
<td>Accounts Receivable</td>
<td>RREV</td>
<td>0.00</td>
<td>77,777.77</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>------------</td>
<td>-----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>77,777.77</td>
<td>77,777.77</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applied Distributions</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Document Number</td>
<td>Apply Date</td>
<td>Discount</td>
<td>Write off</td>
<td>Amount Applied</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>INV03009</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>999.99</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>SLS121012</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>2,249.70</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>SLS11015</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>832.32</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>SLS11016</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>5,000.00</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>SLS20000</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>2,461.00</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>STDINV2227</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>171.10</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>STDINV2228</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>128.30</td>
<td></td>
</tr>
<tr>
<td>SLS</td>
<td>STDINV2252</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>5,702.69</td>
<td></td>
</tr>
<tr>
<td>DR</td>
<td>DM20020</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>2,500.00</td>
<td></td>
</tr>
<tr>
<td>FIN</td>
<td>FC20010</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>20.00</td>
<td></td>
</tr>
<tr>
<td>SVC</td>
<td>SVC1000</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>468.70</td>
<td></td>
</tr>
<tr>
<td>SVC</td>
<td>SVC10001</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>2,155.79</td>
<td></td>
</tr>
<tr>
<td>SVC</td>
<td>SVC11004</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>1,859.03</td>
<td></td>
</tr>
<tr>
<td>SVC</td>
<td>SVC11013</td>
<td>4/12/2017</td>
<td>0.00</td>
<td>0.00</td>
<td>2,356.59</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>26,840.06</td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$77,777.77</td>
<td>$0.00</td>
<td>$0.00</td>
<td>$50,337.71</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Other Fraud Attacks

• Mass Steal Banking Information
• Mass Steal Credit Card Data
• Private Financial Records
Accounting Controls to Prevent Fraud
Bank Reconciliation

• Timing is everything
• Bank reconciliation compares the bank balance with the book balance monthly
Accounting Controls

• Matching Checks Cut to Invoices
• Matching Address on Check to Address on Invoice
• Process for Adding Vendors to System
• Customer On-Boarding Process
• Confirmation of Vendor Banking Information
• Account Reconciliations
Conclusions
What about Technical Controls?

• Never discount “Defense-in-Depth”

• All it takes is for one control to fail!
  – GP, SQL server, user permissions/roles, security awareness, antivirus, IDS, incident response

• This is why the accounting controls are more important to implement
Final Thoughts

• It is possible to perpetrate fraud against the accounting system from the outside
• Fraud is much easier for an insider
• Combine malware with legitimate entries = perfect crime
• Combination of technical and accounting controls are required to combat modern fraud
Questions?

• **Tom Eston**
  teston@securestate.com
  Twitter: agent0x0
  Blog: Spylogic.net

• **Brett Kimmell**
  bkimmell@securestate.com
  Twitter: kimmellbrett

• More details on attacks included in our whitepaper