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

Tom Eston – SecureState
teston@securestate.com

Brett Kimmell, CPA – SecureState
bkimmell@securestate.com
# Table of Contents

- Introduction .................................................................................................................................................................. 3
- Locating and Dissecting the Accounting Systems ........................................................................................................ 4
- Traditional Examples of Accounting Fraud .................................................................................................................. 4
- Overview of Microsoft Dynamics Great Plains .............................................................................................................. 5
- Dynamics GP Users ................................................................................................................................................... 6
  - Microsoft SQL Server SA (System Administrator) Account .................................................................................... 6
  - Other Accounts ....................................................................................................................................................... 6
  - Current Versions of GP ........................................................................................................................................... 7
- Locating Microsoft Dynamics GP Systems and Database .................................................................................................. 7
- Vulnerabilities and Attack Vectors in Microsoft Dynamics GP ........................................................................................... 8
  - Vulnerabilities found in Microsoft Dynamics GP ........................................................................................................ 8
  - Attacking the Database ............................................................................................................................................ 8
  - Attacking the Microsoft Dynamics GP User ............................................................................................................... 10
  - Creating the Perfect Fraud via Custom Malware ......................................................................................................... 11
- The Attacks: How Fraud Can be Committed .................................................................................................................. 12
  - Manipulating Existing Vendor Records .................................................................................................................... 12
    - Remit to Address .................................................................................................................................................. 12
  - Creating a New Vendor and Manual Check Entry (Mayhem PoC) ........................................................................... 16
  - Changing General Ledger Accounting Records ........................................................................................................ 17
  - Increase Customer Credit Limit ................................................................................................................................ 17
  - Credit Balance in Customer Account, Get a Refund .................................................................................................... 19
  - Miscellaneous .......................................................................................................................................................... 23
- Accounting Controls to Prevent Fraud ......................................................................................................................... 24
  - Bank Reconciliation .................................................................................................................................................... 24
  - Matching Checks Cut to Invoices ............................................................................................................................... 24
  - Matching Address on Check to Address on Invoice .................................................................................................. 24
  - Process for Adding Vendors to System ........................................................................................................................ 25
  - Customer On boarding Process .................................................................................................................................. 25
  - Periodic Confirmation of Vendor Banking Information ................................................................................................ 25
  - Trial Balance is Always in Balance ................................................................................................................................ 25
  - Account Reconciliations ........................................................................................................................................... 26
- A Note about Technical Controls ..................................................................................................................................... 26
- Conclusions .................................................................................................................................................................. 26
- Appendix – Miscellaneous Database Table Name Reference ............................................................................................... 27
- Appendix – Miscellaneous Screenshots ................................................................................................................................ 28
- Credits ......................................................................................................................................................................... 29
- References ................................................................................................................................................................... 29
**Introduction**

Breaking into a company’s internal network is a trivial task for most moderately skilled penetration testers and attackers. The typical methodology usually begins with finding the “low hanging fruit” such as weak Windows domain passwords, open Apache Tomcat and JBoss administration interfaces and the penetration testers’ best friend, the exploitation of the elusive MS08-067 vulnerability. Once administrator level accounts have been compromised, the attacker starts looking for data on company systems. The standard fare usually includes employee passwords, SSNs, PCI cardholder data, PHI, and other data items deemed sensitive or confidential by the company. Typically, this data is found on file shares, email systems and of course, databases. Aside from a screenshot or two of the sensitive information, it’s very rare to find penetration testers provide a proof of concept attack to show the damage that gaining access to this information could do. What separates the moderately skilled penetration tester from the expert penetration tester is finding and showing the manipulation of the accounting and financial systems of the company. If an attacker can control and manipulate the accounting system of the company to commit mass systems fraud, it can create more devastating and long term consequences for the company. Changing or manipulating financial data is just the beginning. As professional penetration testers, we must demonstrate more advanced attacks to show real impact to the business.

In addition to controlling the information systems through technical security controls to ensure confidentiality, integrity and availability; accounting information must be controlled to ensure accuracy, timeliness, relevancy, reliability, consistency and comparability. The backend accounting controls may or may not be in place to ensure these characteristics. This whitepaper will demonstrate one type of attack that would be very difficult for technical security controls to detect. Detecting advanced attacks like these created by technical means relies on the accounting controls instead of the technical security controls.

Moreover, is the accounting staff capable of implementing a set of controls that would detect fraud when resources are limited in many small and midsized companies? Companies in this range of size regularly make decisions on how resources are consumed. For example, they must frequently determine which accounts must be reconciled monthly, quarterly, semiannually, and annually. Whether the lack of resources is a matter of limited skillset or limited time, it is certain that small to midsized companies lack total control over their financial processes. Given the volume of accounts in a typical accounting General Ledger, it is unlikely accounting departments are reconciling every account each month. Based on our experience doing audit work and in discussions with professionals currently in the financial audit area, we estimate roughly 50% of small companies either don’t reconcile their bank accounts or don’t do it properly. This is the most critical control to detect check fraud.

This whitepaper will demonstrate that even with proper bank reconciliation, funds can be diverted without immediate detection. Fraud attacks like the ones described in this whitepaper could last for months or years. Getting caught depends on the skills and resources available and whether an audit is performed or not. Included in the following sections is a comprehensive look at how to attack a financial system using advanced technical and manual means which could be used to pull off the “perfect heist”.
Locating and Dissecting the Accounting Systems
Locating the accounting systems on an internal network and knowing the intricacies of how they work is frequently overlooked by penetration testers. These systems can include a mixture of front end web servers, client systems and databases. Through our research we’ve found that accounting systems like Microsoft Dynamics Great Plains are typically installed with very specific identifying information. This information includes server names, database tables and other valuable information. If an attacker knows how to identify these sensitive systems it becomes very easy to find out what data to manipulate and what changes need to be made to commit fraud. This whitepaper will highlight the typical naming conventions, database structure and other details from the popular Microsoft Dynamics Great Plains accounting system. These are beginning steps required for any of the attacks discussed in the later sections of this whitepaper.

Traditional Examples of Accounting Fraud
Accounting fraud (aka: deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit) in the traditional sense can encompass several areas. Frauds can range from insider embezzlement and overstating profits to external check fraud. Insider fraud could be a kickback scheme, skimming, over and under stating balances to meet goals or sales fraud. One of the more common external frauds against a company is bank fraud. A typical example of this is taking money from the company’s checking account by fraudulent check or wire. This type of fraud occurs frequently and is successful because of lack of internal controls. Fraud investigators find that companies are not reconciling their bank accounts properly which is the primary control to detect bank fraud. The one similarity all frauds share is that diversion of amounts recorded on the books should lead to unsubstantiated account balances. While there are some controls built into accounting systems, such as a trial balance, other controls must be implemented to properly protect funds.

Every so often you read in the media about the accounting clerk that has been taking money out of the company Christmas fund and paying themselves thousands of dollars a year. For example, in 2009 a 43 year old woman was caught writing checks against her boss’ personal checking account in Akron, Ohio. She had been doing it for eight years and stole more than $1.78 million from his checking account. In this case he obviously did not reconcile his checking account1. In October 2012, a man bought $3,360 of product from a Lowes with a counterfeit check and then returned the goods for gift cards. The victim discovered the fraud when he reconciled his bank account. In this instance, there was a check drawn on the bank and no record of the check on his books. $3,360 was probably a good percentage of the man’s checking account balance, and the fraudulent check likely stood out like a flashing red light2.
Overview of Microsoft Dynamics Great Plains

This whitepaper will be focusing on the most popular accounting system for medium to large size (middle market) businesses, Microsoft Dynamics Great Plains (GP). Companies and governments large and small from all over the world are using Microsoft Dynamics ERP products. For example, at the annual “Convergence 2012” conference, Microsoft announced 11 new customers to an already growing list of 1,000 public-sector organizations across the United States3. GP has the ability to do more than financial management. Its modules can be used for business intelligence, supply chain management, payroll, human resources and more4. GP was originally an independent company located in North Dakota called Great Plains Software. Microsoft purchased the company in late 2000 for $1.1 billion dollars5. GP is written in the Dexterity programming language6 which was specifically designed for the GP product.

Figure 1: Great Plains Software in 1989 7

GP was designed for a “client-server” architecture. Meaning, the application requires a client installation to run on the user workstations. The application itself and required components are installed on the client. The client then communicates to the GP database (see Figure 2 below). A web front end, called GP Business Portal, is also an optional installation with GP; however, this requires Microsoft SharePoint in order for this feature to be functional. GP Business Portal is also limited in terms of data input functionality. For example, you cannot enter journal entries or enter vouchers with GP Business Portal8. GP Business Portal is primarily designed for querying information and reporting.
Dynamics GP Users
One of the more interesting features of GP is that there is no integration with Windows Active Directory (note Figure 2 above). All user accounts are created, managed and stored in the Microsoft SQL Server GP database. Active Directory integration requires the installation of third-party add-on components.

Microsoft SQL Server SA (System Administrator) Account
The main account used to install the GP database is the “SA” database account. This account is the most critical account because it can log in to the GP application as well as the SQL server database. The “SA” account is also required for adding users within the GP application when GP is first installed. While newer versions of Microsoft SQL Server (2008 and above) recommend disabling the SA account, the SA account is required by GP for installation as well as for the application to run. If the SQL server is misconfigured and the security of the SA password is compromised, the GP database will be compromised as well. For example, it’s typical that most SQL servers have Domain Administrators added to the Local Administrators group on the SQL server for maintenance and administrative tasks. This Local Administrator group is also sometimes added to the “sysadmin” role on the SQL server. In a typical internal network attack once a Domain Administrator account is compromised, the databases are usually compromised as well. This is the most popular way to compromise the GP database directly.

Other Accounts
Besides the “SA” account, there are several other accounts that are used by GP that are of interest to an attacker. A fantastic blog post by JP Davey is referenced in the research below which gives very good context to the purpose of these accounts in GP.

DYNSA
DYNSA is the account that owns all GP databases. This account allows GP to perform privileged administrative and maintenance tasks without using the “SA” user account. DYNSA is created during the GP installation and can only log in to the GP application, not the database directly.
System Password
The system password is created during the installation of GP. This password is required when performing GP security tasks, multicurrency access and other items. The interesting thing to note about the system password is that when logging into GP with DYNSA or SA you still need to provide this password when doing certain GP security tasks. The same rules apply for non-privileged GP accounts. You still need the system password to do these tasks regardless of the privilege level of the GP account. Microsoft provides the system password functionality as an additional layer of security.

Dynamics GP Users
Last but not least are the regular GP users. These are the accounts used to perform all the tasks required by accountants, controllers, payables, receivables and more. As mentioned previously, these accounts are not Windows Active Directory accounts (domain level accounts). GP user accounts are created by the SA user or by a GP administrator account that has been assigned roles via database permissions. What’s important to note is that by compromising a Windows Active Directory account’s (domain user) password, an attacker should utilize this same password if the user is found to be using Dynamics GP. As previous research has shown, users typically reuse the same password for multiple sites and systems. For example, by compromising the Windows Active Directory account of the corporate controller, this user may have significant privileges in the GP application for conducting many of the fraud attacks detailed in this whitepaper.

Current Versions of GP
The most current version of GP as of this whitepaper is Microsoft Dynamics GP 2010 R2 (11.0 SP2) which was released May 1, 2011. This whitepaper will focus on GP 10.0 which is the most common version being used by companies today.

Locating Microsoft Dynamics GP Systems and Database
The first step in attacking GP is to locate the systems and database. Typically, system administrators will have system naming conventions that indicate that a GP system is in use. Most Windows based networks can be easily queried for internal DNS information once a foothold in Active Directory is achieved or system names can be identified using a tool such as “nbtscan” (found in the BackTrack 5 security tool distribution). Example naming conventions for GP systems typically include some or all of the following names:

- GP
- GP-PORTAL
- DYNAMICS
- DYNAMICS_DB
- GREAT PLAINS
- ACCOUNTING
- FINANCE
In addition, company Intranet pages will typically have links and instructions for accessing GP. If a company is using Microsoft SharePoint this can lead to finding the GP Business Portal (if being used).

Once the GP systems are identified, the next step is to conduct additional reconnaissance to determine what systems are being used. The most critical server to locate is the GP database server; however, the business portal and any client installations are also valuable targets because the compromise of these systems will lead an attacker quite easily to the GP database server. Later in this whitepaper we will look at attacking the GP client directly through a malicious process injection attack called “Mayhem”.

**Vulnerabilities and Attack Vectors in Microsoft Dynamics GP**

**Vulnerabilities found in Microsoft Dynamics GP**
There have been a few remote overflow vulnerabilities and one denial of service issue in Dynamics GP version 9 and lower. Through our research we haven’t identified any exploit code available for the vulnerabilities listed below:

- **Microsoft Dynamics GP DPS Message Invalid Magic Number Remote DoS**
  http://osvdb.org/show/osvdb/48819

- **Microsoft Dynamics GP DPM Component DPM Message Remote Overflow**
  http://osvdb.org/show/osvdb/48820

- **Microsoft Dynamics GP DPS Component DPS Message Remote Overflow**
  http://osvdb.org/show/osvdb/48821

The only recent Dynamics GP vulnerability identified (in 2010) was regarding a weak cipher being used for encrypting the system password. This issue was later debunked by Microsoft. While the cipher is weak the system password itself is more of an additional layer of security for some of the administrative functions within GP. Once an attacker has access to the SQL server and the Dynamics GP database the system password is not needed.

For our purposes, in this whitepaper the attacks we describe require access to the Dynamics SQL database from the SQL server or access to a Dynamics GP client system by either authenticating to GP as a valid user (via account hijack) or by a process injection attack.

**Attacking the Database**
The ultimate goal for an attacker is to modify the Dynamics GP database to create and modify entries to commit various fraud attacks. One way to do this is to modify the GP database tables directly. However, we need to know how the GP database tables are named and structured so we know what to modify. To the untrained eye GP database tables are not very descriptive without a reference of some kind. Figure 3 below shows the naming structure of a Dynamics GP database from the view of the Microsoft SQL Enterprise Manager.
To properly identify the tables needed to commit fraud, an attacker would need to reference the following chart that was created by Dynamics GP consultant Leslie Vail on her blog “Dynamics Confessions”\textsuperscript{16}.

<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>

Figure 3: Example of Dynamics GP Database Tables

Figure 4: Dynamics GP Table Naming Conventions
A further list of other miscellaneous table identifiers is provided in the appendix of this whitepaper. Once the table is identified there is also a five digit number which identifies the table type. This list (also from Leslie Vail’s blog) is provided below.

<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>

Figure 5: Dynamics GP Table Number Identifiers

Matching these two pieces together allows the attacker to determine the type of fraud they want to commit. For example, PM1000 would reference the Payables Management work table. This table could be used in the manipulation of vendor records. We describe this attack in more detail in the committing fraud section later in this whitepaper.

**Attacking the Microsoft Dynamics GP User**

The users of GP are a focus of many of the attacks described in this whitepaper, specifically the accounting department users, controller, bookkeeper, CFO and others. Besides compromising the user’s GP username and password, the more sophisticated attacker will want to compromise the PC of the victim. Once the PC is compromised from a targeted attack, malware (in this case, Mayhem) would be installed on the victim’s PC to allow a backdoor process injection attack. This attack is described in detail in the next section.

A typical attack scenario that could be used to attack the GP users would be a targeted spear phishing attack. For example, the attacker gathers GP users though user information (name and email address) from job titles found on the social network LinkedIn. Next, a phishing email is created that would convince users to click a link or download a malicious attachment. Once the victim is compromised the Mayhem malware would be installed and would begin to target the GP processes. There are also other scenarios that could be used, including compromising other users of the company and using those systems as pivot points to locate GP users. Other techniques that would be used in standard internal penetration testing methodologies such as PTES\(^7\) (Penetration Testing Execution Standard) can also be utilized once access to the internal network is obtained.
Creating the Perfect Fraud via Custom Malware

What if this fraud could be undetectable by our traditional computer security controls such as antivirus and IDS (Intrusion Detection Systems) as well as the non-technical accounting controls? What savvy attacker hasn’t wanted to create a fraud attack as demonstrated in the popular cult classic film “Office Space”? Install a virus via a floppy disk, the virus attacks the accounting system to shave off a fraction of a penny of each transaction. Check the account balance via the ATM and profit.

The attacks described in this whitepaper are made practical through proof of concept code published in conjunction with this research. The research on attacking GP in this manner and proof of concept code was created by Spencer McIntyre of the SecureState Research & Innovation Team. The proof of concept code, which is affectionately named “Mayhem”, utilizes standard malware techniques such as function hooking and library injection to execute within the context of the Dynamics GP front end. The goal is for the malware to open a channel back to a malicious attacker and allow them to issue commands specific to GP through the Dynamics GUI frontend. The proof of concept code needs to be injected at run time but well known patching techniques could be employed to have the necessary components loaded at run time.

When the malware is installed it creates hooks in key locations to intercept function calls to and from various components of the application. The most important hooks are the ones that intercept calls to the ODBC32 library. The malware monitors for calls that allocate handles for interacting with the database and create their own by duplicating the function calls. The result is a valid set of handles specific to the malware that can be used for injection of SQL commands into the database as the authenticated user. By creating additional handles to interact with the database the malware can initiate actions regardless of the state of Dynamics GP as a whole. This also has the added benefit of not relying on passwords and allowing actions to be executed on behalf of the authenticated user.

One of the hooks is installed to intercept the ODBC32.SQLConnect function. This handler makes the call to the original SQLConnect function and checks that the connection was successfully made. Once the connection is made the handle is duplicated and a new thread is spawned to run in the background. The
new thread makes requests via HTTP to the attacker’s server and waits for commands such as SQL statements to be executed. This allows the attacker a semi-covert channel by which to interact with GP while the legitimate user’s session is parasitized.

The Attacks: How Fraud Can be Committed
The purpose of this section is to present a few different frauds that can be committed, assuming the perpetrator has gained appropriate access levels to Dynamics, either via malware such as Mayhem, direct access to the Dynamics SQL database or directly into the Dynamics front end application. These attack methods concentrate on fraud that would divert money out of a company via the checking account. Companies potentially could be victims of multiple fraud types, but a frequent fraud against a company is bank fraud. Therefore, we have concentrated our research on identifying attack vectors for this type of fraud, and later, identify controls to help prevent these types of frauds.

Manipulating Existing Vendor Records
Remit to Address
Vendors may have several addresses, ship-to, mail-to, and remit-to addresses. In addition there are ship-to for products, mail-to for regular mail, and remit-to for checks. A simple SQL update query in GP can add a remit-to address or change an existing vendor’s remit-to address. For example in Figure 7 below, the VADCDRTO has been changed to “BRETTKIMMELL” which is the remit-to address record containing Brett Kimmell’s address and not Company X’s. When the funds are processed for payment, the check is mailed to Brett Kimmell instead of the vendor. Obviously, the vendor will be looking for payment at some point so this type of fraud has a limited life span and would be more practical for a single attempt.

Figure 7: PM Paid Transaction History File with Remit-To Field
In Figure 8 below, the remit-to address reference has been changed to BRETTKIMMELL inside of GP with no issue or alarms being sounded by Dynamics. It is important to understand this field is just a reference to a record in another table. Whatever address is associated with that record will be the address the check is mailed to.

![Figure 8 Vendor Detail Information in GP Where Addresses Can be Changed](image)

It is also possible to edit an existing vendor remit-to address instead of adding a new record. Below, the table in Figure 9 shows how the table containing different vendor addresses is structured. Each VENDORID can be listed multiple times and have multiple ADRSCODE. The last record shown has the code BRETTKIMMELL as the address code to use for BEAUMONT0001 when sending a check.

![Vendor address table showing multiple address codes](image)
In Figure 10 below, an existing vendor’s remit-to address is updated with simple SQL. It’s not hard to think of all the SQL Update queries that could be executed by an attacker.

Figure 10: The Vendor WESTJUNC0001 Remit-To Address is Updated Using SQL

In Figure 11 below, the results of the update query are shown in Dynamics. Once again there were no issues with the front end of Dynamics accepting an update query through the DB manager.
In addition to the remit-to address, the vendor Payee Name can be changed, as seen in Figure 12 VNDCHKNM and Figure 8 Check Name. The Vendor Check Name VNDCHKNM field is located in the PM Vendor Master File.
Creating a New Vendor and Manual Check Entry (Mayhem PoC)
The attacker may create a new vendor in GP and add an invoice or simply distribute the debit to an expense account at the time of posting. GP has the built in functionality to allow manual checks to be entered into the checking account (Figure 13). This feature is available for companies to use when the check printer is broken or the AP clerk is on vacation and there is no backup. Checks can be hand written then entered via the “Manual Payments Screen”. This screen allows the user to post the check along with check number to the checking account detail (Figure 14). If an attacker can get access to this screen or capability via malware like Mayhem, the bank account reconciliation should balance and no attention would be called to a check that exists both in the bank detail and books detail.

Figure 13: Manual Check Entry Screen, No Invoice Needed

Figure 14: Distribution Screen for Manual Check Entry
There is a remote chance that if the fraudster is able to get a new vendor added into the system, an invoice may get paid if mailed in and if the company has extremely poor controls over its disbursement process. Most companies require an approved purchase order or purchase requisition for purchases over a certain amount.

**Changing General Ledger Accounting Records**
Manipulating historical accounting records would cause a company great pains. For an attacker that wanted to be malicious, this would be a simple but effective attack. For example, if the company records are not backed up and the changes were significant enough, the company may not be able to pass their annual audit. Balance sheet account balances are a point in time and represent everything that has happened in that account since its inception. Income statement accounts are a summary of what has happened since the start of the most recent period. Changing balances in accounts for periods that are considered closed would create a nightmare for a company. It is likely the company would have great difficulty and possibly not be able to substantiate balances at the end of the year.

**Increase Customer Credit Limit**
In Figure 15 below, the system reminds the user that some customers are over their credit limit. Figure 15 shows seven customers to be exact in this example. Imagine for a moment that you are in charge of adding new customers and extending credit. There would be a process of customer application, reference verification and credit review. This entire process could be circumvented if given adequate level of permission.

---

**Figure 15: Seven Customers are Over Their Limit**
The Dreaded Credit Limit…Let’s Increase That a Bit
For an existing customer the fraud would be rather easy. SQL update query to PM00200 CRLMTDLR and make sure the CREDLMT=2 as discussed below Figure 12. The attacker could also set CREDLMT=1 which would give the customer unlimited credit.

![Figure 16](image1.png)
**Figure 16** Customer Credit Limit Screen in GP

![Figure 17](image2.png)
**Figure 17**: Customer Credit Limit Table in GP (two different customers)
Credit Balance in Customer Account, Get a Refund

Depending on the company’s process for making refunds of overpayments and credit balances, it may be possible to create an account that looks like it has been overpaid by a customer. With a little social engineering a check would be cut to the customer, clearing out the overpayment. In Figure 18 below a payment was processed through the company’s cash receipt process and resulted in a credit balance. Dynamics has a process for paying back overpaid customers. The option with the least amount of control is “Credit Balance Customers”. Any customer with a credit balance gets a check. In the hopes a company is lacking control over this process, an attacker could create a new customer, add a fake cash receipt which would create a credit balance in the New Customer’s account. In the Figure 18 below, the Credit Balance Option is selected and customer AARONFIT001 has an overpaid balance of $53,505.71. One thing to note, the customer AARONFIT001’s vendor name is EVILVENDOR. Any checks cut would be to EVILVENDOR. The attacker would have less than 30 days to pull this off.

![Figure 18: GP Screen to Process Refund Checks on Customer Overpayments](image-url)
The $53,505.71 is a return for $2,568.00 and an overpayment of $50,937.71. See Figure 19 below.

![Figure 19 Cash Receipt Detail Applying $77,777.77 to Open Receivables](image1)

This is the detail of the $53,937.71.

![Figure 20: Detail of Customer AARONFIT0001's Credit Balance](image2)
Once the clerk starts the refund process, Figure 21 is presented. GP puts the money in a suspense account or wash account. It backs out the overpayment in receivables and temporarily lets it sit in the cash suspense account. It is important to understand this process because the receivables are tracked in the GL (General Ledger) and in the receivable management system (Figure 18). At the end of any period both balances should agree. In Figure 21 the funds are taken from the suspense account and entered into payables. When paid, payables are reduced and cash is reduced.
Cash is King: Who's Wearing Your Crown?

Figure 22: Credit Balance Moving from AR-1200 to Cash Suspense-1190

Figure 23: Credit Balance Moving from Cash Suspense-1190 to AP-2100
In Figure 24 below, the actual check printed by the system is shown. Notice, our esteemed attacker has demonstrated that the vendor Check Name can be changed. He has updated it to be his name.

![Figure 24: Vendor Check Name Changed to the Attacker](image)

**Miscellaneous**

**Mass Steal Banking Information**
Organized crime might be interested in landing bank account information. Depending on the size of the company this could be thousands of bank accounts. Banking information in GP is not encrypted.

**Mass Steal Credit Card Data Stored in the Accounting System**
Customer credit cards are stored in GP and are charged when customers purchase goods. It is possible this information is at risk.

**Private Financial Records**
Any financial information could be considered confidential. Financial statements, account balances and payroll records are typically confidential to the company. A company’s image may be damaged if this information is released to the public. Not to mention employee SSN’s and bank accounts used for direct deposit of payroll.
Accounting Controls to Prevent Fraud

Bank Reconciliation
Timing is everything when it comes to fraud prevention. Bank reconciliation in its simplest form compares the bank balance with the book balance usually at the end of a month. If the balances agree, the account reconciles. There of course can be differences; outstanding checks for example, would be reflected on the books but not on the bank. Typical bank reconciliation also nets debits and credits together as the comparison is of ending balances and not the transactions occurring during the month.

A better way to reconcile the bank account is a four column proof of cash. A four column proof of cash compares the beginning balances, the debits, the credits, and the ending balance. In a simple bank reconciliation, a debit for $10,000 would offset a credit for $10,000. In a four column proof of cash it would be apparent there was $10,000 more in debits on the books and $10,000 more in credits on the books. Timing is an issue, if the check is on the books but has not cleared the bank it would be a reconciling item. A check fraudulently written against a company’s account would typically be discovered during bank reconciliation. If a company doesn’t reconcile its bank account (and there are plenty companies who do not) they would not immediately catch a fraudulent check, but the more the thief stole, the more likely he would get caught. As long as the company was big enough and the thief was not greedy it is likely the fraud could go on for some time.

How could a thief perpetrate a check fraud and not get caught? A fraudulent check is less detectable if the bank account reconciles. The thief could use malware similar to Mayhem, which would make sure the check that was written is on the books. There are a couple of controls that might detect this type of fraud. Positive pay, which is a file of “checks produced” sent to the bank for verification prior to the check being cleared. The second method would be verifying, for each check clearing the bank, whether the check agrees to supporting documentation. Depending on timing, the positive pay file created may include the manually entered check in the listing. The second option is very time consuming and companies typically don’t have the resources to monitor this.

Matching Checks Cut to Invoices
The first question non-accountants ask is “why don’t you just send an invoice to the company”. The answer is that the invoice won’t get paid. Invoices are typically matched with some form of approval document like a purchase requisition or a purchase order. Some companies have a manager sign off on the invoices to validate the purchase. Invoices are scrutinized. There are probably a few companies that pay whatever comes in the front door, but they are few in numbers.

Matching Address on Check to Address on Invoice
One of the simple attacks we discovered was a SQL update query to a vendor’s Remit-To address. This would be good for one or two checks before the vendor was calling looking for payment. For a company to prevent this type of fraud they would have to verify the Remit-To address on each check each time they ran a payout. Alternatively, a tool could be installed to monitor the vendor address table for changes.
Process for Adding Vendors to System
Adding a vendor to the system should be a monitored process. Once a vendor is in a system it gives the vendor some legitimacy. Typically, vendors are given a vendor account number that is chronological and new vendors are at the top of the list with the largest ID number. Most companies do not do a good job monitoring this process and have too many employees with the ability to add new vendors. New vendors should go through an authorization process and active vendors should be recertified each year. Employees authorized to add a new vendor should be limited to a few and any changes should be logged.

Customer On boarding Process
New customers must be approved before being sold to on credit. They should be required to fill out an application, have trade references and their credit reviewed. Once this information is found acceptable to company standards, the new customer would be entered into the system. The accountant needs to protect against a bogus customer being entered into the system. Roles can be used inside the accounting application giving only certain employees the ability to enter new customers. To protect against an attack into the GP database, the company must implement other controls. These controls include reviewing existing customers on a periodic basis against original applications and other documentation.

Periodic Confirmation of Vendor Banking Information
It is fairly common for vendors to be paid via ACH funds transfer. This process saves company’s significant processing time over cutting a traditional check. In order for a vendor to be paid in this manner, they must provide banking information to the remitting company. This leaves room for two types of fraud. First, a skilled attacker could easily download the vendor banking information stored in the GP table. Second, a simple update query can change the vendor’s banking information to the fraudster’s. More than likely a vendor company would come calling a week or two after not receiving payment; however, it would be a good idea to periodically confirm vendor account details in case banking information was changed. A perpetrator could change the banking information in mass for several vendors for a quick material payday. To counter this, the accountant could verify the bank account numbers being paid in the ACH are in fact legitimate vendor bank account numbers by tracing them back to original documentation.

Trial Balance is Always in Balance
One thing about accounting, there are always two sides to every entry and as a result, debits always equal credits. This is reflected in the Trial Balance which adds up all the debits in all the accounts with debit balances and all the credits in all the accounts with credit balances. No matter the period of time you analyze this data, the total debits will equal the total credits. If an attacker goes into a table to make an entry and it does not have an offsetting debit or credit, the fraud will be found out quickly.
Account Reconciliations
Assuming the attacker gains access, installs malware such as Mayhem and is able to get a manual check entry created, that debit would need to go someplace. Every transaction in every account should be able to be substantiated (supported by documentation of some type). Most small to medium sized companies do not reconcile every account each month. They will concentrate on the larger accounts on the balance sheet. Typically, expense accounts are managed via a budget. Unless an expense amount is way off for a month the detail will not be reviewed. Even during an audit, some accounts are not reviewed by the auditing firm.

A Note about Technical Controls
It may be very difficult to catch the fraud attacks that this whitepaper has described by technical means; however, that doesn’t discount that the standard technical security controls need to be applied. GP installation, SQL database configuration, least privilege user permissions, end-user security awareness, antivirus and intrusion detection controls all play a huge part in preventing accounting fraud committed through technical means. Unfortunately, this also means that if one of these controls fails the entire GP system can be compromised by a dedicated attacker. Defense in depth and incident response are more important than ever. Any technical controls implemented need to be working in conjunction with the non-technical accounting controls to properly prevent these attacks from occurring.

Conclusions
Although not a trivial task, it is possible to perpetrate a fraud against an accounting system from the outside. An insider would have a much easier job and a higher likelihood of success. We have shown that with the proper skills and tools a fraud can be committed and that accounting and IT systems are at risk. It takes a combination of technical and accounting controls to detect or prevent fraud. Those companies ignoring this risk leave themselves exposed to great danger of becoming victims.
# Appendix – Miscellaneous Database Table Name Reference

<table>
<thead>
<tr>
<th>Physical Name</th>
<th>Display Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM90000</td>
<td>CM Transmission Log</td>
</tr>
<tr>
<td>CM90001</td>
<td>Checkbook EFT Log</td>
</tr>
<tr>
<td>CN90000</td>
<td>Collections - User Preferences</td>
</tr>
<tr>
<td>ERB90100</td>
<td>Data Connection Products</td>
</tr>
<tr>
<td>ERB90200</td>
<td>Data Connection Series</td>
</tr>
<tr>
<td>ERB90300</td>
<td>Data Connections</td>
</tr>
<tr>
<td>ERB90400</td>
<td>Data Connection Restrictions</td>
</tr>
<tr>
<td>ERB90450</td>
<td>Data Connection Restriction Values</td>
</tr>
<tr>
<td>ERB90500</td>
<td>Data Connection Security</td>
</tr>
<tr>
<td>EXT90101</td>
<td>Product List</td>
</tr>
<tr>
<td>EXT90101</td>
<td>Resource Cache - Product List</td>
</tr>
<tr>
<td>EXT90102</td>
<td>Product Series List</td>
</tr>
<tr>
<td>EXT90102</td>
<td>Resource Cache - Product Series List</td>
</tr>
<tr>
<td>EXT90103</td>
<td>Form List</td>
</tr>
<tr>
<td>EXT90103</td>
<td>Resource Cache - Form List</td>
</tr>
<tr>
<td>EXT90104</td>
<td>Window List</td>
</tr>
<tr>
<td>EXT90105</td>
<td>Report List</td>
</tr>
<tr>
<td>EXT90106</td>
<td>Resource Cache - Table List</td>
</tr>
<tr>
<td>EXT90106</td>
<td>Table List</td>
</tr>
<tr>
<td>PA91301</td>
<td>PA Contract Segment Override Header</td>
</tr>
<tr>
<td>PA91304</td>
<td>PA Contract Segment Override Detail</td>
</tr>
<tr>
<td>PA92301</td>
<td>PA Contract Template Seg Override Header</td>
</tr>
<tr>
<td>PA92304</td>
<td>PA Contract Template Seg Override Detail</td>
</tr>
<tr>
<td>PDK90003</td>
<td>PDK File Error Log</td>
</tr>
<tr>
<td>PDK90100</td>
<td>PDK Security</td>
</tr>
<tr>
<td>PP900000</td>
<td>Deferral Opened Periods</td>
</tr>
<tr>
<td>PTO90000</td>
<td>PTO Pending Master Conversion</td>
</tr>
<tr>
<td>SE90001</td>
<td>Account Rollups Account List Accelerator</td>
</tr>
<tr>
<td>SE988977</td>
<td>Account Rollups Options Columns</td>
</tr>
<tr>
<td>SLB90000</td>
<td>Third Party GoTo Types</td>
</tr>
<tr>
<td>SY90000</td>
<td>SY_User,Object_Store (Dynamics User Object Store)</td>
</tr>
<tr>
<td>SY90100</td>
<td>Default Chart of Accounts</td>
</tr>
</tbody>
</table>
Appendix – Miscellaneous Screenshots

Figure 25: Screen shot showing bank account numbers in Dynamics in clear text

Figure 26: Employee bank account numbers used for payroll direct deposit in plain text.

Customer Bank Accounts

Employee Bank Account #'s From MS///

The field in the script above (DDAMTDLR) will change the dollar amount, DDTRANUM would update the routing number, and DDACTNUM will update the account number. In all cases, once you make the change, you can regenerate the file and the footer information (totals, hash info, etc.) will be correct. To view the contents in the table, use SELECT * FROM DD10500 and you can find the correct dex_row_ID of the record you want to update. You will notice that the records in the table are identified with the build number from the Generate ACH window (field INDEX1 in the table).
Cash is King: Who’s Wearing Your Crown?

Figure 27: Location where Dynamics stores the payroll direct deposit file to be transferred to bank.

Credits

Special thanks to the following people who helped with the development of this research:
Drayton Graham, Brian Dillon, Chris Makley, Matt Neely, Spencer McIntyre and Ken Stasiak.

References

5 http://en.wikipedia.org/wiki/Microsoft_Dynamics_GP
6 http://en.wikipedia.org/wiki/Dexterity_programming_language
8 http://www.slideshare.net/JeffreyPaulette/business-portal-for-dynamics-gp
9 http://download.microsoft.com/download/8/F/A/8FABACD7-803E-40FC-ADF8-355E7D218F4C/SQL_Server_2012_Security_Best_Practice_Whitepaper_Apr2012.docx
12 http://www.pcmag.com/article/219303/password_use_very_common_research_shows.html
13 http://www.backtrack-linux.org/
14 http://www.christopherkois.com/?p=448
16 http://dynamicsconfeessions.blogspot.com/2012/05/data-flow-and-table-names.html
18 Office Space ©1999 Twentieth Century Fox
19 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. Note Figure 17 below.