Comp 401
Assertions Practical Example and The Importance of Being Earnest

Instructor: Prasun Dewan
Prerequisite

- Assertions (Preconditions and Postconditions)
public class ABankAccount implements BankAccount {
    int currentBalance = 0;
    public static final int MIN_BALANCE = 100;
    public ABankAccount (int initialBalance) {
        currentBalance = initialBalance;
    }
    public int getCurrentBalance () {return currentBalance;}
    public void deposit (int amount) {currentBalance += amount;}
    public boolean withdraw (int amount) {
        int minNecessaryBalance = MIN_BALANCE + amount;
        if (minNecessaryBalance <= currentBalance) {
            currentBalance -= amount;
            return true;
        } else return false;
    }
}
USING WITHDRAW

[ABankAccount]

Current Balance
2500

Withdraw ...
Safe Withdraw ...
Deposits

Parameters of Withdraw

File
Parameter 1: int 2400

[Boolean]

File Edit View Customize Boolean Comparable


WITHDRAWING one DOLLAR: NOT ALLOWED BECAUSE of MIN BALANCE requirement
WITHDRAWING A LARGE AMOUNT: ALLOWED

Parameters of Withdraw

File

Parameter 1: int 2147483647

Withdraw

Integer.MAX_INT
RESULTING BALANCE

![Current Balance](image)

-2147483547
INTEGER OVERFLOW

Most significant bit of positive (negative) numbers is 0(1)
public boolean safeWithdraw (int amount) {
    assert amount > 0: "amount < 0";
    boolean retVal = withdraw(amount);
    assert currentBalance >= MIN_BALANCE: "currentBalance < MIN_BALANCE";
    return retVal;
}
Using Safe Withdraw with MaxInt: The Importance of Being Earnest
### INTEGER OVERFLOW IN REAL LIFE

#### Security Issues - Gain
Description, integer overflow in memory allocation results in heap overflow. By passing the size variable as -1, integer overflows to 0 when 1 is added in...
egain.sourceforge.net/security/?id=2 - 7k - Cached - Similar pages

#### Gentoo Linux Documentation -- Samba Integer overflow

#### The KOffice Project - XPDF Integer Overflow 2
KOffice 1.3 (including betas) to 1.3.5 have an integer overflow vulnerability in KWord's PDF. References, the corresponding security advisory for KOE...
koffice.org/security/2004_xpdf_integer_overflow_2.php - 9k - Cached - Similar pages

#### Microsoft Windows LoadImage API Function Integer Overflow
Microsoft Windows is reported prone to a remote integer overflow vulnerability...
securityresponse.symantec.com/avcenter/security/Content/12095.html - 26k - Cached - Similar pages

#### CERT Advisory CA-2002-25 Integer Overflow In XDR Library
There is an integer overflow present in the xdr_array() function...
cert.org/advisories/CA-2002-25.html - 26k - Cached - Similar pages

#### [LSS | Security | eXposed by LSS | Details]
mod_auth_radius remote integer overflow. Advisory ID: LSS-2005-01-02...
security.lss.hr/index.php?page=details&id=LSS-2005-01-02 - 16k - Cached - Similar pages

#### Network Security, Vulnerability Assessment, Intrusion Prevention
eEye - Network security & vulnerability management software including...
Although the copy length is similarly subject to an integer overflow...
eveye.com/html/research/advisories/KB20051108a.html - 16k - Nov 20, 2005 - Cached - Similar pages

#### Network Security, Vulnerability Assessment, Intrusion Prevention
For the purpose of signature development and further security research, a sample...