Attack Progressions

First they came for bandwidth...
Now they want to make a difference

Steve Riley
Technical Director, CTO Office
steve.riley@riverbed.com
Menu

- Who are the bad guys?
- Why is software insecure?
- How bad are the threats?
- How expensive are attacks?
- What’s going on?
- What’s particularly troubling?
- Is there a pattern that can help us?
- What should we be doing?
Prelude
Short history of “hacking”

Operating System Services
- Buffer overruns, XSS
- Web spoofs, worms

Application Services
- SQL injection, SQL Slammer
- Media players

Eavesdropping
- DES, AES, IPSec

Network Protocols
- Syn flood, DNS spoofing

Network Stacks
- “Ping of death”

Emanations
- Tempest

Insiders
- TCSEC, Common Criteria
Understanding the landscape

- National Interest
- Personal Gain
- Personal Fame
- Curiosity

Tools created by experts now used by less skilled attackers and criminals

Fastest growing segment

- Spy
- Author
- Expert
- Specialist
- Hobbyist Hacker
- Vandal
- Thief
<table>
<thead>
<tr>
<th>WE</th>
<th>THEY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fix all</strong></td>
<td><strong>Find one</strong></td>
</tr>
<tr>
<td>Protect all</td>
<td>Attack one</td>
</tr>
<tr>
<td>Rare</td>
<td>Common</td>
</tr>
<tr>
<td>A lot</td>
<td>Not much</td>
</tr>
<tr>
<td>Limited</td>
<td>Infinite</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Victims</td>
</tr>
<tr>
<td>Automation</td>
<td>Work to do</td>
</tr>
<tr>
<td>Time to do it</td>
<td>Infinite</td>
</tr>
</tbody>
</table>
The fundamental problem
(examples later)

Intended Behavior

Traditional Bugs

Security Bugs

Actual Behavior
Traditional methods are no longer effective.
Attack progressions

Confidentiality

Integrity

Non-repudiation
The future isn’t what it used to be...
You don’t have time

Low Client Impact

- Vendor updates; email notices; CERT subscriptions
- Automatic patch management tools

High Client Impact

- SEIM scanning and policy modification
- Port shutdowns

% Vulnerable Clients

- 30% in 24 hours
- 20% in 48 hours
- 5% in 24 days
- 3% in 7 days (Port shutdowns begin)
- 2% in 24 days

24 days average to 98% secured
Current days to exploit = 3 days

7 Days – SMS Forced patching begins for normal cycle
7 Days – Port shutdowns begin
Choose the type of breaches to display:

- **Unintended disclosure (DISC)** - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or other means.
- **Hacking or malware (HACK)** - Electronic entry by an outside party, malware, and spyware.
- **Payment Card Fraud (CARD)** - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
- **Insider (INSID)** - Someone with legitimate access intentionally breaches information, such as an employee or contractor.
- **Physical loss (PHYS)** - Lost, discarded or stolen non-electronic records, such as paper documents.
- **Portable device (PORT)** - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
- **Stationary device (STAT)** - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
- **Unknown or other (UNKN)**

Select organization type(s):

- BSO - Businesses - Other
- BSF - Businesses - Financial
- BSR - Businesses - Retail/Merchant
- EDU - Educational Institutions
- GOV - Government and Military
- MED - Healthcare - Medical Providers
- NGO - Nonprofit Organizations

Select year(s):

- 2005
- 2006
- 2007
- 2008
- 2009
- 2010
- 2011
- 2012
- 2013

Click or unclick the boxes then select Go.

Breach Total

608,183,147 RECORDS BREACHED

(Please see explanation about this total.)

from 3,788 DATA BREACHES made public since 2005

http://www.privacyrights.org/data-breach/
2011 Cost of Data Breach Study: United States

March 5, 2012, 12:00 am
(click to download study) Symantec Corporation and Ponemon Institute are pleased to present 2011 Cost of Data Breach Study: United States, our seventh annual benchmark study concerning the cost of data breach incidents for U.S.-based companies. While Ponemon Institute research indicates that data breaches continue to have serious financial consequences for organizations, there is evidence that organizations are becoming better at managing the costs incurred to respond and resolve a data breach incident. In this year’s study, the average per capita cost of data breach has declined from $214 to $194.

2011 Cost of Data Breach Study: United States

Benchmark Research sponsored by Symantec
Independently Conducted by Ponemon Institute LLC
March 2012

608,183,147 \times \$194.00 = \$117,987,530,518
608,183,147
×
$194.00

$117,987,530,518

Can’t we do better?
1,179,875,305 barrels of oil
(at $100/bbl.)

9,111,006 four-year degrees
($12,950 for one year tuition at Univ WA, 2013)

190,641 HIVer lives saved
($618,900 lifetime, Nov. 2006 Medical Care)

9,493,686 families/yr fed
($239/wk for 2 adults and 2 children, USDA 2013)
Caught with pants down, again

**We fiddle with**

- CRM
- Records Mgmt.
- Inv. / Shipping
- Order Mgmt.

**Bad guys target**

- CRM Protocol
- Inventory Protocol
- Data Retention Protocol
- Checkout Protocol
Some data
Industry-wide vuln disclosures

- Cf. 2009, avg 3,500 per H
Vulnerability severity

- Based on CVSS scores
Exploit types

- No auto-update = very, very bad
Windows vs. Android

- Won’t always be this way
Android malware growth

- Kaspersky predicts even more
Infection by country, 3Q12
Infection by country, 4Q12
Threat categories

- Autorun—shut it off, please
- Whatever happened to spyware?
Phishing sites, 3Q12
Phishing sites, 4Q12
Spam blocked, 1H09-2H12

- Cutwail and Rustock botnets taken down
Malware distribution, 3Q12
Malware distribution, 4Q12
What worries me
Fun with Android

- XSS in AirDroid allows DoS against host
- Send malicious SMS to premium-rate numbers to steal money
- Siphon data with Wi-Fi tether software, Shark for Root, and OpenVPN
- SIM destruction from visiting infected website

Now more popular than Windows for malware authors (Kaspersky Labs)
BYOD

=

weak platform

+

oblivious users
People as targets

- **8 - human**
  - Figure it out on your own
  - Minimal training exposure (few minutes a year)
  - Quickly forgotten or ignored
  - Unpredictable

- **7 - application**
- **6 - presentation**
- **5 - session**
- **4 - transport**
- **3 - network**
- **2 - link**
- **1 - physical**
  - Written code
  - Thoroughly tested (including penetration)
  - Updated regularly
  - Functions only as designed
Targeted: Spear phishing

- Criminals bombard businesses with targeted spam that looks and feels like internal messaging
  - Think...how did they learn the formatting and style...?
- Usually spoofs IT and HR
- Duped people reveal credentials; attackers easily get inside
- Great for attacking small organizations
Targeted: Watering hole

- Attackers inject malware into website whose typical visitors are the target audience
- Plant multiple tools, including log harvesters
- Popular among hacktivists and those plotting espionage
Botnets: frighteningly successful

- Low interest rates!
- Gimme credit cards!
- Extend your body parts!
- Get a better job!
- Cheap movie tickets!
An affiliates program

“Our first program pays you $0.50 for every validated free-trial registrant your website sends to [bleep]. Commissions are quick and easy because we pay you when people sign up for our three-day free-trial. Since [bleep] doesn’t require a credit card number or outside verification service to use the free trial, generating revenue is a snap.

The second program we offer is our pay per sign-up plan. This program allows you to earn a percentage on every converted (paying) member who joins [bleep]. You could make up to 60% of each membership fee from people you direct to join the site.

Lastly, [bleep] offers a two tier program in addition to our other plans. If you successfully refer another webmaster to our site and they open an affiliate account, you begin earning money from their traffic as well! The second tier pays $0.02 per free-trial registrant or up to 3% of their sign-ups.”
Let’s do the math

$BOTNET$ spams 100,000,000 mailboxes. What if...

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Action Description</th>
<th>Number of Mailboxes</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>Read email and clicked link</td>
<td>10,000,000</td>
<td>$50,000</td>
</tr>
<tr>
<td>1%</td>
<td>Signed up for a three-day trial</td>
<td>100,000</td>
<td>$144</td>
</tr>
<tr>
<td>1%</td>
<td>Enrolled for 1 year</td>
<td>1,000</td>
<td>$144,000</td>
</tr>
</tbody>
</table>

Would **YOU** do it???
Vulnerability chaining

MWR Labs Pwn2Own 2013 Write-up - Webkit Exploit

Recently, MWR Labs took part in the Pwn2Own 2013 competition in Vancouver, demonstrating a full sandbox bypass exploit against Google Chrome (1). The exploit used two vulnerabilities:

- A type confusion in WebKit, Chrome’s rendering engine at the time (CVE-2013-0912)
- A kernel pool overflow in Microsoft Windows, the underlying operating system

- Escaped sandboxed renderer
- Acquired elevated privileges
- Bypassed ASLR and DEP
- Executed arbitrary code

http://labs.mwrinfosecurity.com/blog/2013/04/19/mwr-labs-pwn2own-2013-write-up---webkit-exploit/
DoS attacks popular again

- **THC SSL DoS**
  rapid key renegotiation

- **R.U.D.Y. (R U Dead Yet?)**
  slow rate HTTP POST, server hangs while waiting for long form input to complete

- **Slowloris**
  trickle feed of HTTP headers over several simultaneous connections

- **Sockstress**
  overtake host with perpetually stalled connections
Attacks against integrity

Ukrainian Hacker Makes a Killing in Stock Market Fraud
By Kim Zetter  February 15, 2008 | 3:23:01 PM  Categories: Crime

The NY Times has an interesting story today that’s indicative of an emerging hacking-for-profit trend that just might allow the perpetrator to keep his ill-gotten gains. In this case, the crime doesn’t involve hacking databases to steal credit and debit card numbers, but hacking a computer to obtain inside information in order to profit on the stock market.

The case involves a Ukrainian engineering consultant named Oleksandr Doroshko who is about to be charged with hacking into a computer network that contained advance information of a negative earnings announcement for IMS Health, a company that provides market research to the pharmaceutical and health care industries. [*Correction: An earlier version of this post said that the computer Doroshko hacked belonged to IMS Health. Court records show that Doroshko actually hacked the computer network of Thomson Financial to obtain the earnings information.*]

Doroshko apparently obtained the information just a few hours before IMS, on October 24, announced a significant reduction in earnings, that would drop within three days. Doroshko invested about $42,000 in the options, an amount that nearly equals his annual income, estimated to be between $45,000 and $50,000.

Hours later, IMS Health announced that its earnings had dropped 15 percent from the previous year and 28 percent below analysts’ expectations. Doroshko’s put options on IMS Health, purchased at $30 each, would drop within three days. Doroshko’s put options on IMS Health, purchased at $30 each, would drop within three days. Doroshko’s put options on IMS Health, purchased at $30 each, would drop within three days.

The broker, Interactive Brokers, suspected something was wrong and temporarily froze the money to investigate before Doroshko could withdraw it. Now the Securities and Exchange Commission wants to seize the funds, but a federal judge has ruled that the freezing of the money was unlawful because Doroshko didn’t violate the securities law governing insider trading.

http://blog.wired.com/27bstroke6/2008/02/ukrainian-hacle.html
Veterans given wrong drug doses due to glitch

About 50 medical centers reported problems with electronic health records

The Associated Press

updated 11:46 a.m. PT, Wed., Jan. 14, 2009

WASHINGTON - The top Republican on the House Veterans Affairs Committee demanded Wednesday that the VA explain how it allowed software glitches to put the medical care of patients at its health centers nationwide at risk.

"I am deeply concerned about the consequences on patient care that could have resulted from these mistakes being made without being disclosed to patients who were directly affected," said Rep. Steve Buyer, R-Ind. "This would have enabled the VA to analyze all of its pertinent records to determine if any veterans were harmed, and I would like to know who was responsible for the testing and authorized the release of the new application."

Patients at VA health centers were given incorrect doses of drugs, had needed treatments delayed and may have been exposed to other medical errors due to the glitches that showed faulty displays of their electronic health records, according to internal documents obtained by The Associated Press under the Freedom of Information Act.

Undisclosed problems
The glitches, which began in August and lingered until last month, were not disclosed to patients by the VA even though they sometimes involved prolonged infusions for drugs such as blood-thinning heparin, which can be life-threatening in excessive doses.

In one case, a patient having chest pains at the VA medical center in Durham, N.C., was given heparin for 11 hours longer than necessary as doctors sought to rule out a heart attack.

The goal of electronic medical records nationwide is to help avert millions of medical mistakes attributed in part to paper systems, such as poorly written prescriptions. But health care experts say the VA's problems illustrate the need for close monitoring.

Veterans groups were also harshly critical, saying the VA's secrecy created a false sense of security.

"It's very serious potentially," said Dr. Jeffrey A. Linder, an assistant professor of medicine at Harvard Medical School who has studied electronic health systems. "There's a lot of hype out there about electronic health records, that there is some unfettered good. It's a big piece of the puzzle, but they're not magic. There is also a potential for unintended consequences."

Wrong patients
The VA's recent glitches involved medical data — vital signs, lab results, active meds — that sometimes popped up under another patient's name on the computer screen. Records also failed to clearly display a doctor's stop order for a treatment, leading to reported cases of unnecessary doses of intravenous drugs such as blood-thinning heparin.

The VA said there were nine reported cases in which patients at VA medical centers in Milwaukee, Durham, N.C., and Marion, Ind., were given incorrect doses, six of them involving heparin drips for patients with chest pain. The other cases involved infusions of either sodium chloride or dextrose mixtures that were prolonged for up to 15 hours past the doctor's prescribed deadline.

The agency noted that veterans with questions or concerns can request a copy of their medical record at any time, such as via the "My Healthevét" online system at www.myhealth.va.gov.

http://www.msnbc.msn.com/id/28655104/
Attackers follow a pattern

First they came for bandwidth by attacking availability. They executed denial of service attacks starting in the mid 1990s and monetized later with extortion.

Next they came for secrets by attacking confidentiality. They disclosed sensitive data starting in the late 1990s and monetized with personally identifiable information and accounts for sale in the underground.

Now they’re coming to make a difference by attacking integrity. They degraded information starting at the beginning of the 2000s. These attacks will manifest as changes to trusted data such that those alterations benefit the party making the change. This sort of attack undermines the trustworthiness of data.

What to do
Attack progressions

Confidentiality

Encryption

Integrity

Availability
Think like a bad guy
Who would ever attack us?

- You have **data**, you have a **net** connection
  - *Therefore, you are interesting*
- Hire some testers who are good at **breaking things** (*maybe your kids?*)
  - Think about how your code could be abused
- Build **resiliency** and **protection** into your applications
A personal example
No input validation $\rightarrow$ get free stuff

Intended Behavior

Actual Behavior

Traditional Bugs

Security Bugs
Single-layer protection
Reduce the attack surface
Avoid poor user decisions

Warning

The application "foo.exe" is attempting to connect to port 4659 on 169.254.12.37 via port 8934.

Do you wish to allow this? If this is unexpected behavior click No.

Yes  No  Help

Warning

To see the dancing pigs you must make this dialog go away.

Do you want this dialog to go away?

Duh. Of course!  No. Bug me again.  Tell me something I won't understand
Automate everything

- Code vs. config vulns—prevalence?
- Third type—circumvention
- Get the humans out of the process
- CMU study: 95% attacks succeeded because of configuration mistakes
- Consider feedback system for applying automatic policy updates and enforcement
- Patch-then-fix vs. lots of prior testing
Encryption works—use it!

- **Time/cost trade-off**
  - Buy a safe (and its protection level) based on value of contents
  - Consider similar approach to encryption and digital signatures
- **Watch this space**
  - Predicate e.—policy-driven portion access
  - Functional e.—plaintext must satisfy some function (perhaps an identity)
  - Homomorphic e.—do work without decrypting
It's all about the data

- Physical
- Networks
- Hosts
- Applications
- Data
Guiding principles

Trends drive security threats upward

Evolving Security Controls

Data Self-Protection

Anywhere Access

Security of Digital Assets

Network

Host

People and Process

Time
It's all about the data

Data
Applications
Hosts
Networks
Physical

Diagram showing levels of data, applications, hosts, networks, and physical.
Fortsess vs. biology

- “Defense in depth” blah blah blah
- How many layers are enough?
- Biological systems provide “graceful degradation” with some functionality
Stuff to consider

- **Shrink** exposure
- **Consolidate** resources
- **Streamline** processes
- **Standardize** builds and configuration
- **Add redundancy** to mitigate DoS
- **Require authentication** for all access
- **Encrypt/sign data** in storage and in transit
- **Validate** transactions and procedures
- **Audit activity** for accountability and compliance
Yes, it's real work. So start planning now.
Thank you!

Steve Riley
Technical Director, CTO Office
steve.riley@riverbed.com