The Future of Hacking

An Ethical Hacker’s View

Peter Wood
Chief of Operations
First•Base Technologies
Who am I?

• Started in electronics in 1969
• Worked in networked computers since 1976
• Second microcomputer reseller in UK (1980)
• First local area networks in business (1985)
• Founded First•Base Technologies in 1989
• Conceived network security best practice (1991)
• Presented BS 7799 throughout UK for BSI (1997)
• First independent ethical hacking firm in UK
• Founded white-hats.co.uk in 2002
• Times 1000 / FTSE 100 and CNI clients
What is a hacker?

- Someone who plays golf poorly
- A programmer who breaks into computer systems in order to steal or change or destroy information
- A programmer for whom computing is its own reward; may enjoy the challenge of breaking into other computers but does no harm
- One who works hard at boring tasks

[WordWeb.info]

Is that all?
What is hacking?

• Hacking is a way of thinking
  A hacker is someone who thinks outside the box. It's someone who discards conventional wisdom, and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. [Bruce Schneier]

• Hacking applies to all aspects of life and not just computers

• Increasingly, hacking is used to perpetrate crimes – theft, blackmail, terrorism …
Criminal hacking techniques

- Internet intrusion attacks  
  (against web applications, remote access portals)
- Trojans, rootkits, keyloggers et al.  
  (via phishing, cross-site scripting, web sites)
- Botnets and denial of service attacks  
  (primarily for blackmail or political attacks)
- Social engineering & physical attacks  
  (insider attacks, wireless, bluetooth, laptop theft)
Typical response: technology

For web application attacks:

- Direct Internet connection
- Packet filtering
- Stateful firewall
- Application firewall
- Secure code

For remote access attacks:

- Telnet
- SSH
- HTTPS
- VPN
- VPN & 2-Factor Authentication

This becomes an arms race - criminals will seek an easier route ...
The blended attack

Social engineering \textit{plus} technology

Currently:
- Phishing
- Trojans & rootkits
- Laptop theft
- In person intrusion
Why social engineering?

• Social engineering can be used to gain access to any system, irrespective of the platform.

• It’s the hardest form of attack to defend against because hardware and software alone can’t stop it.
Social engineering

- Any medium that provides one-to-one communications between people can be exploited, including face-to-face, telephone and electronic mail. All it takes is to be a good liar.

- Dorothy E. Denning
  Information Warfare and Security
Remote worker hack

1. Buy a pay-as-you-go mobile phone
2. Call the target firm’s switchboard and ask for IT staff names and phone numbers
3. Overcome their security question: *Are you a recruiter?*
4. Call each number until voicemail tells you they are out
5. Call the help desk claiming to be working from home
6. Say you have forgotten your password and need it reset now, as you are going to pick up your kids from school
7. Receive the username and password as a text to your mobile
8. Game over!
IT support hack

1. Get staff contact names and numbers from reception
2. Call a target user who is unlikely to be technical
3. Say you are from IT working on upgrading their servers over the weekend
4. Say you need their username and password to test their account so that all will work smoothly on Monday morning
5. Game over!
In Person

• Be an employee, visitor or maintenance staff
• Look for information lying on desks and overhear conversations
• Do some shoulder surfing
• Plug in a sniffer or keylogger
• Simply use a vacant desk & workstation
Would you let this man into your building?
Key Logger

Time to get admin password = 10 minutes
Keystroke capture

Keystrokes recorded so far is 2706 out of 107250 ...

<PWR><CAD>fsmith<tab><tab>arabella
xxxxx<tab><tab>None<tab><tab>None<tab><tab>None<tab><tab>None<tab><tab>
<CAD> arabella
<CAD>
<CAD> arabella
<CAD>
<CAD> arabella
exit
tracert 192.168.137.240
telnet 192.168.137.240
cisco
A typical response
Preventing blended attacks

All the money spent on software patches, security hardware, and audits could be wasted without prevention of social engineering attacks.

That means investing in staff awareness backed up by policies.
Countermeasures

Physical aspect:
- in the workplace
- over the phone
- dumpster diving
- on-line

Psychological aspect:
- persuasion
- impersonation
- conformity
- friendliness

Combat strategies require action on both the physical and psychological levels
Staff Awareness

- Train all employees - everyone has a role in protecting the organisation and thereby their own jobs
- If someone tries to threaten them or confuse them, it should raise a red flag
- Train new employees as they start
- Give extra security training to security guards, help desk staff, receptionists, telephone operators
- Keep the training up to date and relevant
Workplace Security Policy

- Shred phone lists, email lists and other important documents before throwing away
- Some documents will need to be locked away
- Basic best practice - clear desk policy
End Point Security Policy

- Use screen savers with password controls
- Encrypt information on desktops, laptops and PDAs
- Secure mobiles and PDAs (infrared, bluetooth)
- Secure wireless (strong encryption, short range)
- Physically destroy unused hard disks, CDs and other media
Help Desk Policy

• Password resets only with call-back and PIN authentication
• Incident reporting and response procedures
• Clear escalation procedures
• Help desk staff should be encouraged to withhold support when a call does not feel right. In other words “just say no …..”
Staff Guidance

- What can be discussed over the telephone
- What can be discussed outside the building
- What can be written in an e-mail
- Don’t use e-mail notification or voicemails when away from the office. It sets up the replacement as a target.
- How to report an incident and to whom
Compliance

• Have a security assessment test performed and heed the recommendations
  - Test the company's ability to protect its environment, its ability to detect the attack and its ability to react and repel the attack
  - Have the first test performed when the company is expecting it
  - Do a blind test the second time around
End of Part One
Need more information?

Peter Wood
Chief of Operations
First•Base Technologies

peterw@firstbase.co.uk

http://fbtechies.co.uk
http://white-hats.co.uk
http://peterwood.com
The Real Risks of Stolen Laptops

An Ethical Hacker’s View

Peter Wood
Chief of Operations
First•Base Technologies
Who am I?

• Started in electronics in 1969
• Worked in networked computers since 1976
• Second microcomputer reseller in UK (1980)
• First local area networks in business (1985)
• Founded First•Base Technologies in 1989
• Conceived network security best practice (1991)
• Presented BS 7799 throughout UK for BSI (1997)
• First independent ethical hacking firm in UK
• Founded white-hats.co.uk in 2002
• Times 1000 / FTSE 100 and CNI clients
This Presentation

• All organisations now have laptop users

• Laptops are vulnerable to theft

• This info may help reduce your exposure!
The target - a “corporate” laptop

- What sensitive information can we steal?
- What credentials can we steal?
- Can we connect to the corporate network?
- Can we introduce a Trojan?
Some example objectives

• Company-confidential documents & spreadsheets
• User’s logon
• The local admin logon
• User’s personal data
• User’s VPN logon
• The contents of the corporate network!
Stage 1 – Own the laptop

Start Here

Switch on laptop

Can we boot from CD, diskette or USB?

Yes

Is CMOS password protected?

No

Is Config password protected?

Yes

Change boot sequence

Boot DOS or NTFS Reader

Copy password hashes to USB key

Crack with rainbow tables

Own the laptop

No

Give up

Is hard disk encrypted?

Yes

Move hard disk to spare laptop

No
If we can boot from CD …
Boot Ophcrack Live
We have the passwords!

<table>
<thead>
<tr>
<th>ID</th>
<th>USERNAME/LMHASH</th>
<th>LMpasswd1</th>
<th>LMpasswd2</th>
<th>NTpasswd</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>Administrator</td>
<td>WINDOW5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>501</td>
<td>Guest</td>
<td>/EMPTY/</td>
<td>/EMPTY/</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>SUPPORT_388945a0</td>
<td>/EMPTY/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td>XPADMIN</td>
<td>L0NGH0R</td>
<td>N</td>
<td>L0ngh0rn</td>
</tr>
<tr>
<td>1004</td>
<td>ASPNET</td>
<td>01Z1ANA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1011</td>
<td>HelpAssistant</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1014</td>
<td>LMAadmin</td>
<td>YA6PT3P</td>
<td>J1</td>
<td>yA6pT3pj1</td>
</tr>
</tbody>
</table>
... or just read the disk
Find the password hashes
Copy hashes to USB key
Copy hashes to your cracking PC and plug in the rainbow tables
… a few minutes later
That was the shortest route
No CD boot possible, but we have access to CMOS
Only the hard disk is enabled
Config is password protected, but the hard disk is not
So let’s take out the hard disk …
.. And read it in our laptop!
That was the longer route!
So what now?

- What sensitive information can we steal?
- What credentials can we steal?
- Can we connect to the corporate network?
- Can we introduce a Trojan?
What sensitive information can we steal?

- Almost anything on the hard disk!
  - MS Office passwords are no protection
  - Neither are zip files (usually)
  - Windows EFS may not protect you either

- But we cannot see data that has been encrypted using a proven algorithm (e.g. PGP volumes)
What credentials can we steal?

- Almost anything on the hard disk!
  - All local Windows password hashes
  - Cached Windows logons
  - Dial-up credentials
  - E-mail passwords
  - Cached web credentials
  - Etc.
Can we connect to the corporate network?

- Very probably!
  - We know the local Windows passwords
  - If you use two-factor authentication, where is your SecurID card and PIN kept?
  - Perhaps the help desk will be very helpful?
  - Perhaps we can use a Trojan to get access later
Can we introduce a Trojan?

• Since we are local Administrator, yes!
  - We can turn off anti-virus
  - We can turn off the personal firewall
  - We can hide the Trojan using a rootkit

• Game over!
However ...
If there’s no access to CMOS …

This computer system, #D7531J-595B, is protected by a password authentication system. You cannot access the data on this computer without the correct password.

Please type in the primary or administrator password and press <Enter>.
... and a password-protected disk

Hard-disk #22Z2HW2PB-595B, the system Primary HDD, is protected by a password authentication system. You cannot access data on this hard drive without the correct password.

Please type in the hard-drive password and press <Enter>.
ATA Password Reset

**Overview**

Repair Station is data recovery software which allows you:

- to diagnose and repair system area problems of hard disk drives,
- to remove passwords from drives locked with an ATA-password (security level HIGH or MAXIMUM).
Or … just whole disk encryption
That was the route to failure!
Need more information?

Peter Wood
Chief of Operations
First•Base Technologies

peterw@firstbase.co.uk

http://fbtechies.co.uk
http://white-hats.co.uk
http://peterwood.com