Dealing with Malicious Code a CERT perspective

Graham Ingram
General Manager
AusCERT

Overview

- About AusCERT
- The CERT perspective
- What's the problem?
- Picking the winners
- Changing the paradigm
- Future directions

AusCERT

- Australia's National CERT – a trusted single point of contact
- Independent and "not for profit"
- Formed in 1993 to provide incident response assistance to Australian universities - AARNET
  - after students used university hosts to compromise foreign government networks
- Membership based funding model
  - National and International members
  - Universities, Government, Private sector
- Commonwealth Govt Funding

AusCERT security bulletins

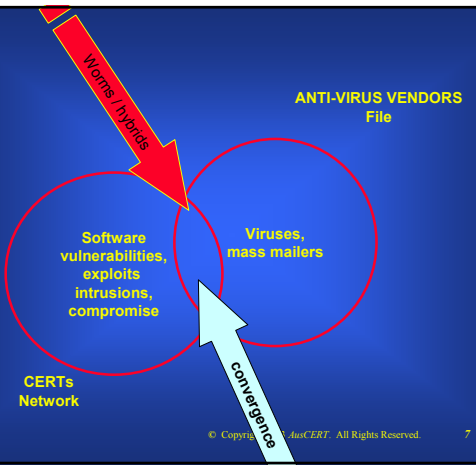
- 99% concern computer network vulnerabilities in hardware devices, software or protocols
- Include bulletins researched and written by AusCERT and those redistributed from other sources, which meet security threshold
- Security threshold – general rule of thumb
  - Provides unauthorised remote access
  - Provides unauthorised privileged access; or
  - Allows an attacker to execute arbitrary code; or
  - Result in a denial of service; and
  - Affects systems in common use

AusCERT

- Advice on Computer Network threats and vulnerabilities
  - Alerts and advisories
- Coordination and handling of computer security incidents
  - National Regional and Global incident handling
  - Vulnerabilities
  - Exploits
  - Intrusions
- Malicious Code
  - Selective – most significant

Malicious Code

- Virus
  - host file/program to propagate
  - Some form of human involvement
- Mass Mailer
  - E-mail propagation
  - Social engineering to execute
- Worm
  - Network enabled propagation
  - Software vulnerabilty exploited to compromise remote host
  - Little or no direct human involvement
- Malicious use of legitimate software or undocumented software "features"



Worm Characteristics:

- Propagation mechanism – to find other hosts to infect
  - Random scanning
  - Subnet scanning
  - Directed scanning
- Vulnerability/Exploit – to compromise remote host
- Payload
  - Backdoors, root kits, DDOS
- Effects – intended or unintended
  - DOS

Worm Issues:

- Propagation/saturation rates
  - Can be faster than defence mechanisms
  - Flash Worms – (<15 minute saturation)
- Payloads
  - Backdoors – DDOS - Executables
  - root kits - spam
- Impacts/Effects
  - DOS, Network Congestion, hardware failure
- Ability to defend
  - Zero day exploits
  - Availability of patches
  - Blended and optimised

Worm Concerns:

- Improved worm engineering
  - Planning Design Testing Delivery
  - Better more efficient programming practices
- More significant Vulnerabilities and faster production of exploits
- Payloads
  - Use of high impact payloads – not seen to date
- Incentives
  - Spam, Cybercrime, State sponsored
- Ability to defend
  - Zero day exploits and availability of patches
  - Blended and optimised - Rootkits

CERT History

- CERT/CC founded to respond to the Morris worm
  - November 2 1988
  - Topographical
  - Exploited buffer overflow in finger daemon
  - Debug command in sendmail
  - Cracked user passwords
  - Used trust relationships between machines
  - No payload
  - Saturation in around 24 hours
  - Numerous bugs and programming problems

AusCERT founded to respond to network intrusions sourced from Australia

What's the problem?

- 80% of organisations were infected with worm, virus or trojan in 2003
  - 76% in 2002
- 57% suffered financial loss as a result
  - 43% in 2002
- Average losses per organisation $17,922 in 2003
  - $11,881 in 2002
- Malicious code infection was the only area which showed increased level of activity in the survey
  - Source: 2003 Australian Computer Crime and Security Survey.

Malicious code threats

- How many?
  - 24 Sept – 22 Oct Symantec reported on 95 new malicious code threats (Cat 1)
  - In 29 days about 3.27 per day
  - About 1193 per year – at current rates
- Which are the most serious?
  - CERTs only interested in the most serious – greatest potential for damage and propagation
    - » In 2001, we reported on 18
    - » In 2002, we reported on 7 (quiet year)
    - » In 2003, we reported on 12 (up until 27 October)
  - With hindsight, some did not prove to be as serious as anticipated

Picking the winners

- CERT goal: to provide early warning advice about malicious code threats
- **In a timely manner**, we want to know which **will** be:
  - the fastest
  - the most virulent
  - the most damaging
  - the most widespread

But . . .

'Early warning' – is it obsolete?

- **Reality**: Most 'warnings' occur after the propagating code has been released
- The speed of propagation means that "warning" may be "early" but still well after extensive compromise
  - Example:
    - » Code Red v2 over 100 hosts infected within 1st hour (CAIDA)
    - » Slammer infected 90% vulnerable hosts within 10 minutes (CAIDA)

Volume and Speed

- Code Red v2
  - 359,000 hosts in < 14 hours
  - Doubled in size every 37 minutes
  - At its peak 2,000 new hosts infected per minute (CAIDA)
- Nimda
  - Compromised 450,000 hosts in first 12 hours (CERT)
- Slammer
  - Achieved full scanning rate (5 million scans per second) within 3 minutes
  - Doubled in size every 8.5 seconds
  - Infected 90% of vulnerable hosts within 10 minutes\
  - Infected at least 120,000 (CAIDA)
- SoBig.F
  - Around 1 million infected emails intercepted in the first 24 hours
  - Around 16 million infected emails (Messagelabs)
  - Estimates of hundreds of thousands of host compromised

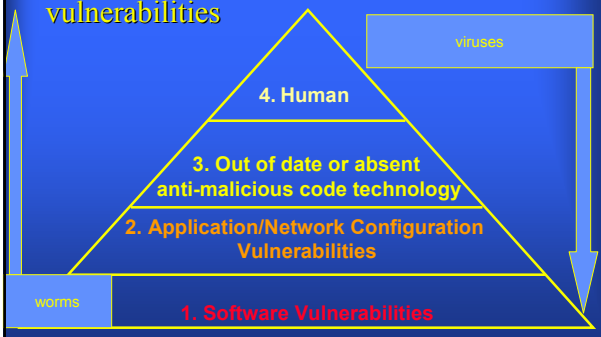
Is early warning obsolete or do we need to change the paradigm?

- ~~Improve early warning or bust~~
- Improve early warning or make it redundant
  - Providing effective early warning, **post code release and BEFORE** compromise occurs is now unlikely
  - Early warning **post code release** is confined to reducing impact and providing recovery advice
- How to make early warning redundant?
  - Focus on providing timely advice on the protection against vulnerabilities
  - This way, early warning occurs **BEFORE code release** and **BEFORE compromise**
- The specific details of the latest malicious code becomes less critical if the fundamentals steps to secure the network are already in place.

Protection against vulnerabilities exploited by malicious code writers

- Software vulnerabilities
  - MSBlaster
  - Welchia
  - Slammer
  - Code Red I & II
  - Slapper
  - Scalper (Apache worm)
- Application configuration vulnerabilities, eg browser, firewall
  - Nimda
  - Slammer
- Inappropriate use (or lack) of malicious code protection technologies
  - SoBig variants
- Human behaviour vulnerabilities
  - Opening executables (social engineering), eg SoBig.F
  - Using weak passwords, eg Spida

Malicious code hierarchy of vulnerabilities



Conclusion

- Early warning after malicious code is released is too late
- Focussing on fixing software vulnerabilities will provide opportunity to protect against the majority of the most serious malicious code threats
- In time, with the prospect of zero-day exploits becoming more common, focusing on the software vulnerabilities will also be too late
  - It's time to focus on secure programming
- Who will be the champions?

How Many is Too Many?

- What does it mean to have 4200 vulnerabilities reported to CERT-CC in 2002?
- Somebody has to read the descriptions of the vulnerabilities
  - » 4200 * 20 minutes to read = 175 days just to read the descriptions.
- • Suppose you're affected by 10%
  - » 420 vuls * 1 hour to install the patch = 52 days just to installpatches on one machine
- • Just to read security news and patch a single system 175 + 52 = 227 days
- • Even just 5 minutes to read new bulletins and a 1% "hit rate"
- costs almost 50 days, or about 20% of a perfectly efficient administrator.

Global initiatives

- APCERT
  - Developing points of contact – sharing incident data
  - Regional cooperation
- AusAID funded CERT training for emerging economies
- APEC TEL
- ASEAN
- FIRST – founding member

National initiatives

- Cybercrime
  - LEA training
  - Australian Computer Crime and Security Survey
  - Guidelines for the management of IT evidence HB 171-2003
- Australian Anti-Virus Research Forum
- Information Systems Security Professional Certification Scheme
- National incident reporting scheme
- National alerts service
- Critical Information Infrastructure Protection

AusCERT's future directions

- Develop near real-time distributed monitoring and analysis capability
  - autonomous router NetFlow data
  - IDS and firewall log data
  - Why?
    - » Vital to become more proactive in developing own early warning data to collect and analyse
- ISACs
  - Need to provide the above capability on an industry by industry basis

AusCERT contact information

24 hour hotline: (07) 3365 4417
(after hours for member emergencies only)

facsimile: (07) 3365 7031

e-Mail: auscert@auscert.org.au .

world wide web: www.auscert.org.au

postal: AusCERT
The University of Queensland
BRISBANE QLD 4072