HACKING AT MACH SPEED!

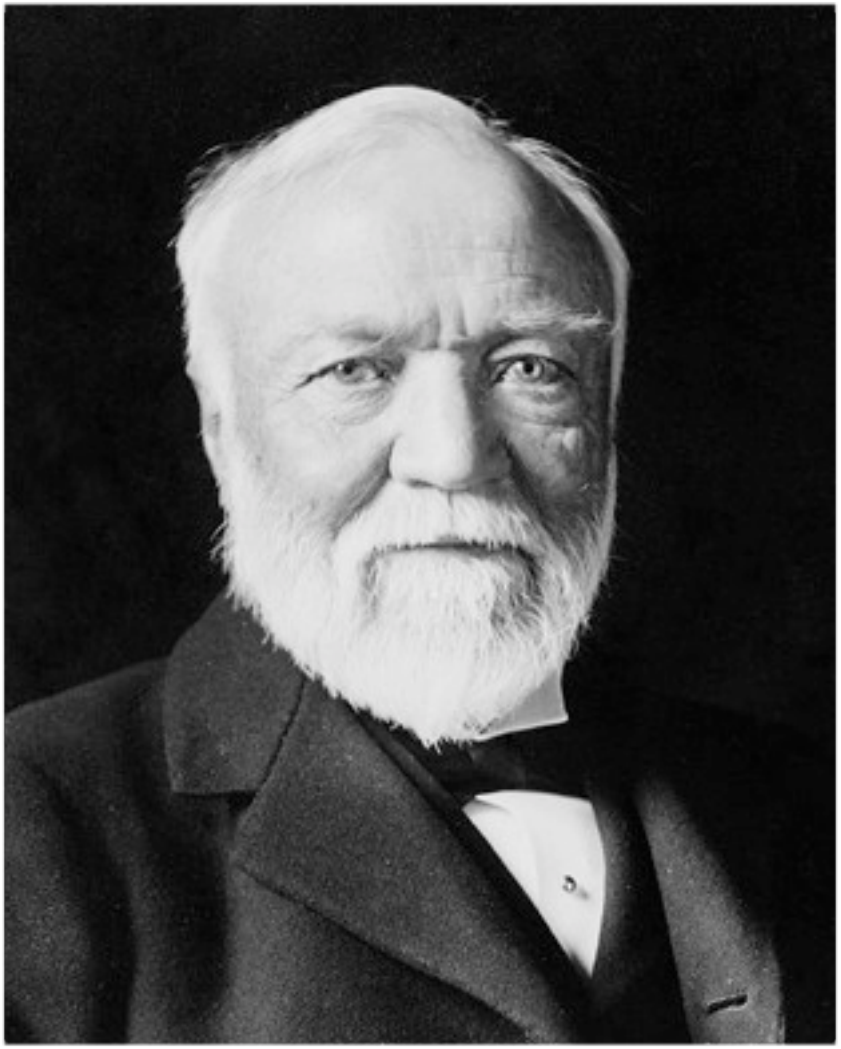
HOW I FOUND AN ODAY AT 9PM THE NIGHT BEFORE SUMMERCON AND SPENT THE REST OF THE NIGHT MAKING SLIDES

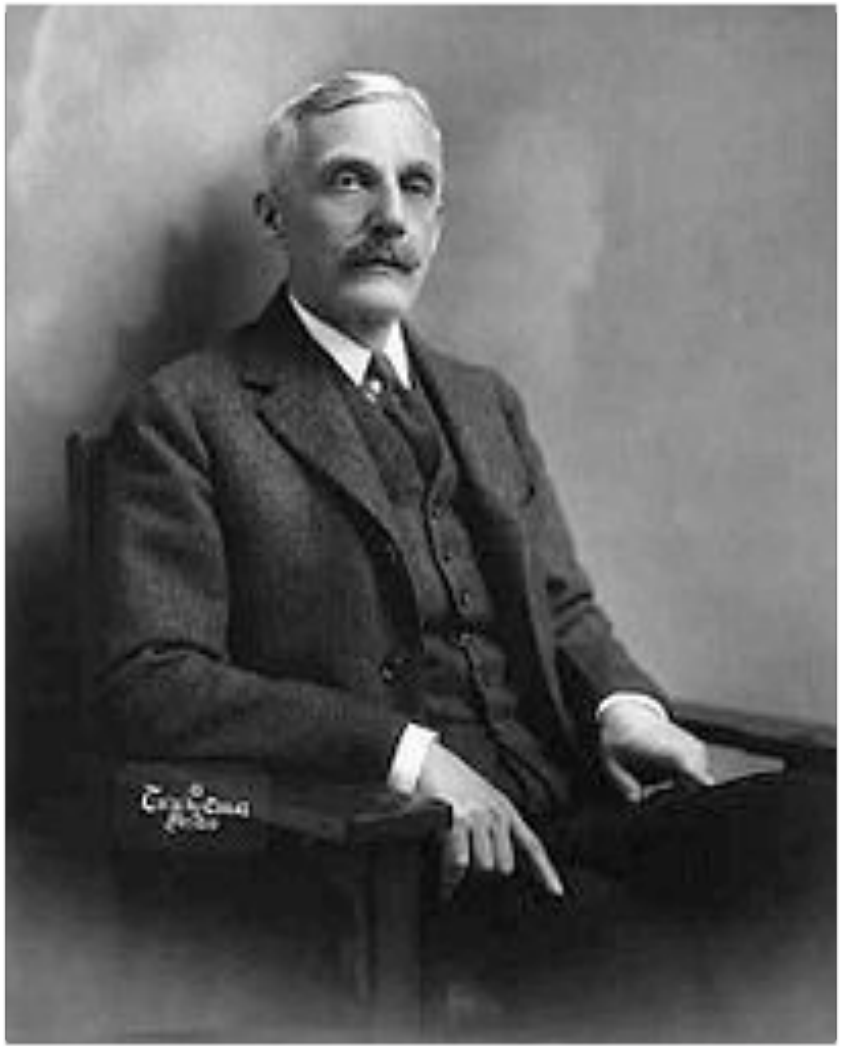
DINO A. DAI ZOVI

@DINODAIZOVI / DDZ@THETA44.ORG

HTTP://TRAILOFBITS.COM / HTTP://THETA44.ORG

INTRODUCTION

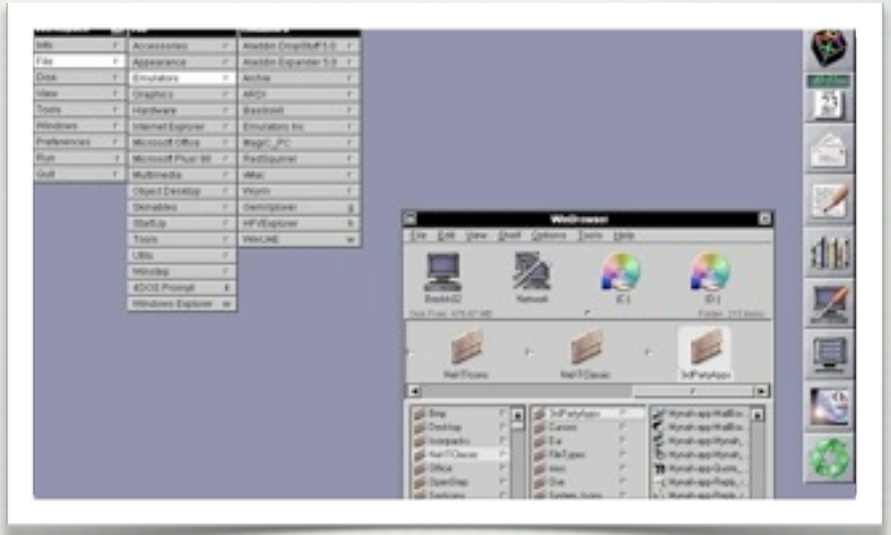




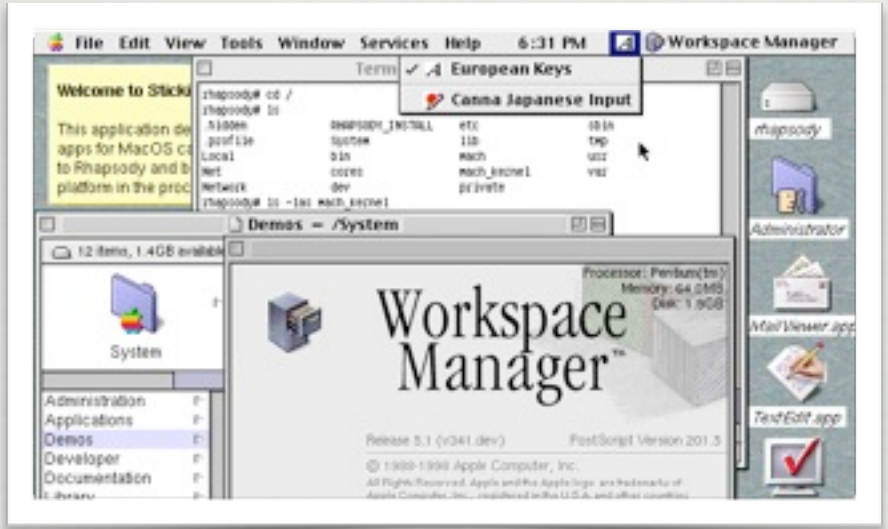
THIS STORY STARTS WITH TWO GUYS NAMED ANDREW,

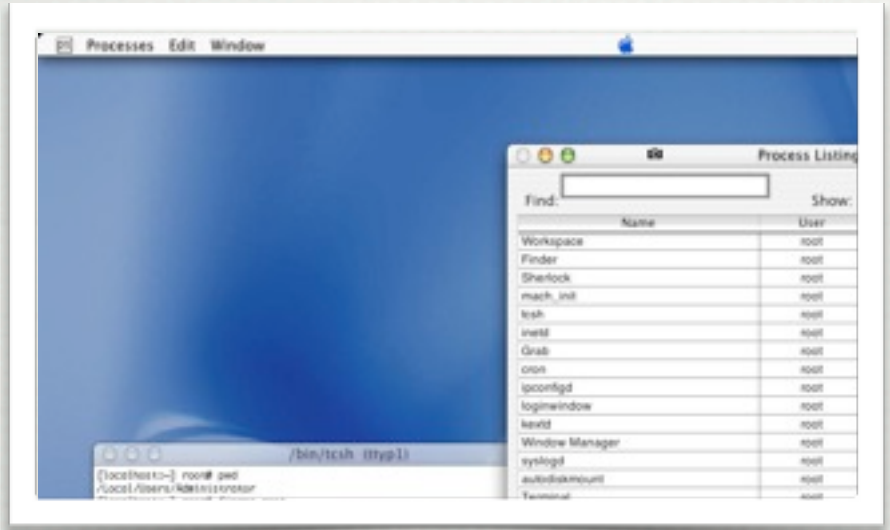
AND THE UNIVERSITY THAT THEY FOUNDED.

CMU GRAD STUDENTS WROTE A MICROKERNEL FOR 4.2BSD/VAX



WHICH WAS USED IN NEXTSTEP





AND NEXTSTEP EVENTUALLY BECAME MAC OS X

THIS MICROKERNEL IS CALLED MACH

WHAT IS ~~LOVE~~ MACH?

WHAT IS IT?

- A MICROKERNEL BASED ON FOUR KEY ABSTRACTIONS:
  - TASKS HOLD RESOURCES AND RUN THREADS
  - A THREAD IS A CONTEXT OF EXECUTION ON A PROCESSOR
  - PORTS ARE UNIDIRECTIONAL QUEUES BETWEEN TASKS
  - MESSAGES ARE STRUCTURED OBJECTS SENT TO PORTS

TASKS

- RESOURCE CONTAINERS THAT HOLD:
  - VIRTUAL MEMORY ADDRESS SPACE
  - ONE OR MORE THREADS
  - PORT SEND AND RECEIVE RIGHTS

THREADS

- REPRESENT A CONTEXT OF EXECUTION ON A CPU
  - VALUES STORED IN EACH CPU REGISTER
  - CPU FLAGS AND OTHER STATE
- MAY BE SCHEDULED TO RUN ON ANY CPU
- MUST BELONG TO ONE AND ONLY ONE TASK

PORTS

- QUEUE OF STRUCTURED MESSAGES
  - VERY UNLIKE UNIX FILE-BASED IPC ABSTRACTIONS
- THE ONE TASK WITH THE EXCLUSIVE RECEIVE RIGHT OWNS IT
- ZERO OR MORE TASKS MAY HOLD SEND RIGHTS TO A PORT
- RIGHTS MAY BE SENT TO OTHER TASKS IN MESSAGES

MESSAGES

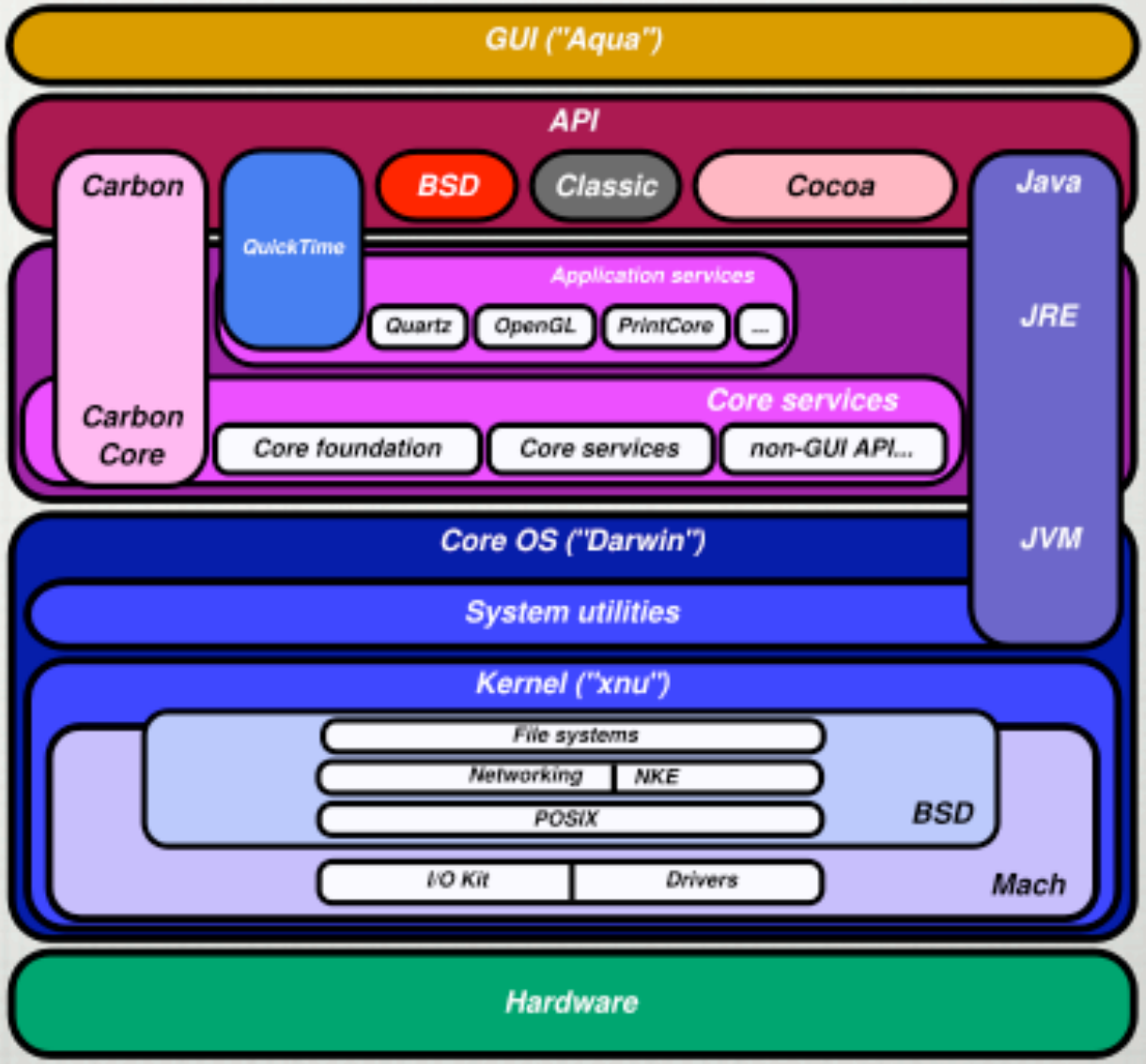
- BASIC UNIT OF INTER-TASK COMMUNICATION
- HEADER SPECIFIES SOURCE/DESTINATION, ETC.
- BODY CONTAINS IN-LINE DATA
  - INTEGERS, STRINGS, FLOATING POINT NUMBERS
- MESSAGE MAY ALSO CONTAIN OUT-OF-LINE DATA
  - PORT RIGHTS
  - MEMORY PAGES

MACH RPC

- MACH RPC IS BUILT USING MESSAGES AND PORTS
- THE MACH INTERFACE GENERATOR (MIG)
  - TAKES A USER-WRITTEN RPC INTERFACE FILE (FOO.DEFS)
  - GENERATES USER AND/OR SERVER STUB ROUTINES THAT ABSTRACT AWAY THE MARSHALING AND COMMUNICATION
  - RPC ROUTINE COMMUNICATION IS ENCODED USING THE SAME FORMAT AS MICROSOFT RPC

WHERE CAN I FIND IT?

SUP DAWG, WE HEARD YOU LIKE KERNELS, SO WE PUT A MICRO-KERNEL IN YOUR KERNEL (SO YOU CAN MACH WHILE YOU BSD)



THE KERNEL IS JUST A TASK

- MOST LOW-LEVEL FUNCTIONS ARE RPC CALLS TO KERNEL
  - TASK, THREAD, MEMORY, SEMAPHORES, ETC
- THE KERNEL IS A TASK, JUST LIKE OTHER PROCESSES ARE
  - CAN READ/WRITE KERNEL MEMORY
  - CREATE, SUSPEND, AND TERMINATE KERNEL THREADS
  - CALL OTHER RPC SERVERS IN THE KERNEL

AUDITING MACH RPC

BOOTSTRAP SERVER

- HOW CLIENTS FIND SERVERS
  - EVERY TASK IS GIVEN SEND RIGHTS TO BOOTSTRAP SERVER'S RPC SERVICE PORT
  - THE BOOTSTRAP SERVER LIVES INSIDE LAUNCHD
- LAUNCH SERVERS ON DEMAND
  - WILL ALSO AUTOMATICALLY RELAUNCH CRASHED ONES

WHERE THE SERVERS AT?

- BOOTSTRAP SERVERS ARE CONFIGURED IN:
  - {/SYSTEM,/,~}/LIBRARY/LAUNCHAGENTS
  - {/SYSTEM,/,~}/LIBRARY/LAUNCHDAEMONS
  - /ETC/MACH_INIT.D
  - /ETC/MACH_INIT_PER_USER.D
  - /ETC/MACH_INIT_PER_LOGIN_SESSION.D
  - DYNAMICALLY USING CALLS TO BOOTSTRAP_REGISTER()

UPDATE_SHARING.DEFS

```
prajna% ls /System/Library/LaunchAgents/
com.apple.AOSNotificationOSX.plist
com.apple.AddressBook.abd.plist
com.apple.AirPortBaseStationAgent.plist
com.apple.AppleGraphicsWarning.plist
com.apple.BezelUI.plist
com.apple.CoreLocationAgent.plist
com.apple.DictionaryPanelHelper.plist
com.apple.Dock.plist
com.apple.FileSyncAgent.plist
com.apple.Finder.plist
com.apple.FontRegistryUIAgent.plist
com.apple.FontValidator.plist
com.apple.FontValidatorConduit.plist
com.apple.FontWorker.plist
com.apple.Kerberos.renew.plist
com.apple.KerberosHelper.LKDCHelper.plist
com.apple.NetworkDiagnostics.plist
com.apple.PCIESlotCheck.plist
[ ... ]
```

BOOTSTRAP_INFO

```
prajna% ./bootstrap_info
ru (Apple)_OpenStep ([0x0-0x27027].com.apple.AppleSpell) = ACTIVE
com.apple.finder.ServiceProvider (com.apple.Finder) = ACTIVE
com.apple.FontRegistry.FontRegistryUIAgent (com.apple.FontRegistryUIAgent) =
ON_DEMAND
com.apple.FontObjectsServer (com.apple.fontd) = ACTIVE
WaveMessagePort.314.23499425 (0x100403990.anonymous.wineloader) = ACTIVE
com.apple.rcd (0x100400510.mach_init.rcd) = ON_DEMAND
com.apple.netauth.useragent (com.apple.netauth.useragent) = ON_DEMAND
com.apple.datadetectors.compiler (com.apple.datadetectors.compiler) =
ON_DEMAND
com.apple.autologinPWHandler (0x100400000.anonymous.loginwindow) = ACTIVE
com.apple.FontWorker (com.apple.FontWorker) = ON_DEMAND
com.apple.Preview.ServiceProvider ([0x0-0x4b04b].com.apple.Preview) = ACTIVE
com.apple.ReportCrash (com.apple.ReportCrash) = ON_DEMAND
com.apple.coreservices.quarantine-resolver (com.apple.coreservices.uiagent) =
ON_DEMAND
com.apple.DictionaryPanelHelper (com.apple.DictionaryPanelHelper) = ON_DEMAND
[ ... ]
```

LET'S GO A BUG-HUNTING

REDACTED

PWN2OWN PRIZES FOR 2012

OR, REPORT YOUR BUGS TO THE VENDORS FOR FREE

VULNERABILITY HANDLING

- WE NEED TO DEBATE "VULNERABILITY HANDLING" NOT "RESPONSIBLE DISCLOSURE"
  - "RESPONSIBLE DISCLOSURE" PRESUPPOSES MANY DECISIONS, JUDGEMENTS, AND INTERESTS
- WAS CREATED FOR 2002'S INTERNET, BUT NOW IT'S 2010
  - MANY OF ZDI'S "UPCOMING ADVISORIES" COULD ENABLE AN "AURORA"-STYLE ATTACK IF EXPLOITED

ARE WE CHASING OUR TAIL?

- ☐ IS THE VULNERABILITY DISCLOSURE STATUS QUO:
  - ☐ AWESOME?
  - ☐ SUFFICIENT?
  - ☐ IRRELEVANT?
  - ☐ A DISTRACTION AT BEST?
  - ☐ ENABLING AN ADDICT?

VULNERABILITIES VS. EXPLOITS

- A VULNERABILITY NEVER OWNED ANYONE, AN EXPLOIT DID
  - THERE ARE MORE PEOPLE THAT CAN FIND VULNERABILITIES THAN CAN WRITE RELIABLE EXPLOITS
  - COUNT NUMBER OF ZDI VULNERABILITY CONTRIBUTORS VS. PWN2OWN CONTESTANTS PAST AND PRESENT
  - A MINORITY OF VULNERABILITIES HAVE THE POTENTIAL TO BE TURNED INTO A DANGEROUS EXPLOIT

EXPLOITS MATTER

- OSVDB QUERY FOR REMOTE VULNERABILITIES IN 2009
  - ~1000 POTENTIAL CODE/COMMAND EXECUTION
- MANUAL ANALYSIS OF EXPLOIT KITS, INCIDENTS, ETC.
  - 40 EXPLOITS OBSERVED BEING USED IN THE WILD
  - MOST COPIED FROM MILWORM WITH FEW CHANGES
    - COMMENT OUT SKAPE/SKYWING DEP BYPASS

BUGS FOR BOSCH

- "GOOGLE ATTACK HIGHLIGHTS 'ZERO-DAY' BLACK MARKET" (AP, 1/29/2010)
  - "I BASICALLY HAD TO MAKE A CHOICE BETWEEN DOING SOMETHING THAT WOULD PROTECT EVERYBODY AND REMODELING MY KITCHEN — AS TERRIBLE AS THAT IS, I MADE THAT CHOICE, AND IT'S HARD," MILLER SAID. "IT'S A LOT OF MONEY FOR SOMEONE TO TURN DOWN."
- ADOBE JBIG2 EXPLOIT WAS SOLD FOR $75K (TWITTER, I THINK)
  - REPORTING BUG RESPONSIBLY FEELS LIKE A MILLION BUCKS!

$75K IS A LOT OF FOOD

- $75K = ~ $512K CNY
- AVERAGE YEARLY SALARY FOR A SOFTWARE ENGINEER IN CHINA IS $90K CNY
  - HTTP://WWW.PAYSCALE.COM/RESEARCH/CN/COUNTRY=CHINA/SALARY
- WOULD YOU "DO THE RIGHT THING" FOR FREE WHEN YOU COULD "DO THE WRONG THING" FOR 5-6 YEARS SALARY?

FIGHTING 0DAY EXPLOITS

- MAKE THEM ILLEGAL!
  - RIGHT... BEST OF LUCK WITH THAT (WTO SANCTIONS?)
- MAKE A TRANSPARENT, OPEN, LEGITIMATE MARKET!
  - VENDORS WILL NEVER PAY OR PLAY ALONG
- MAKE THEM INEFFECTIVE!
  - NOW YOU'RE ONTO SOMETHING...

ONE 0DAY RUINS YOUR DAY

- ONE 0DAY BROWSER OR DOCUMENT READER EXPLOIT IS A SKELETON KEY FOR EVERYONE'S SIDE DOORS
  - THE FRONT DOOR HAS LAYERED FIREWALLS, DMZS, HARDENED SERVERS, INGRESS/EGRESS FILTERING
  - CLIENT DESKTOPS ARE A WILDERNESS OF UNMANAGED OR BARELY MANAGED SYSTEMS WITH SOFTWARE HANDLING UNTRUSTED DATA AS ADMINISTRATOR
  - CLIENT DESKTOPS HAVE UNLIMITED INTERNAL ACCESS

LET'S TALK ABOUT TAVIS

The 15 Most Influential People in Security Today

1 Tavis Ormandy
Google Security Team

As goes Google, so goes Web 2.0 security. Tavis Ormandy, one of the most visible hackers/researchers on the Google Security Team, faces the unenviable responsibility of making sure all of Google's products pass the security smell test. An open-source security guru, Ormandy is tasked with identifying and analyzing vulnerabilities and exploits--and with getting them fixed before the bad guys can do damage. He is also co-lead of the Gentoo Security Team, shoring up the security of the Linux distribution.

NO MORE FREE BUGS

- TAVIS VOLUNTEERED THE HELP CENTER VULNERABILITY TO MICROSOFT
  - BEGGARS CAN'T BE CHOOSERS
- IF VENDORS OFFERED A BUG BOUNTY, THEY CAN SET THE TERMS FOR THE PAYOUT
  - PAY UP FRONT, OFFER A BONUS IF RESEARCHER DOESN'T DISCLOSE ANY INFORMATION BEFORE OFFICIAL ADVISORY
- INCREASING PERCENTAGE OF MICROSOFT PRODUCT VULNERABILITIES ARE BEING REPORTED THROUGH ZDI, IDEFENSE, OR OTHER SIMILAR PROGRAMS

IS THIS THE ADVANCED PERSISTENT THREAT?

OR, "HOW MANY CHINESE HACKERS DOES IT TAKE TO COMPROMISE YOUR NETWORK?"

CYBERWARRIORS OR CYBERPUNKS?

- [ ] STOP FLATTERING YOURSELF, YOUR NETWORK IS TRIVIAL TO OWN
  - [ ] YOUR EMPLOYEES AND THEIR E-MAIL ADDRESSES ARE ENUMERABLE ON SOCIAL NETWORKING SITES?
  - [ ] YOUR EMPLOYEES ANSWER EXTERNAL E-MAIL AND ACCESS INTERNET WEB SITES ON THE SAME MACHINE THAT THEY CREATE OR HANDLE PROPRIETARY IP?
  - [ ] ARE THEIR E-MAIL ADDRESSES FIRSTNAME.LASTNAME@COMPANY.COM?

0DAY ATTACKS != H1N1

- STOP TREATING 0DAY ATTACKS LIKE H1N1
  - PEOPLE ARE GETTING SICK WITH AN UNKNOWN VIRUS, WE MUST RESPOND TO THIS INCIDENT
  - TAKE ANTI-VIRAL MEDICATION TO TREAT INFECTIONS
  - WE HAVE DEVELOPED AN IMMUNIZATION SHOT FOR H1N1, EVERYONE PLEASE GO APPLY IT TO YOURSELVES
- ANY HAND-WRITTEN MALWARE WILL EVADE ANTI-VIRUS
- WE DON'T HAVE A CYBER IMMUNE SYSTEM YET

PUBLIC HEALTH VS. CRIME

- MASS MALWARE AND BOTNETS ARE AN INTERNET PUBLIC HEALTH PROBLEM (CYBERHEALTH?)
  - OPPORTUNISTIC, LOW-SKILL AND ATTENTION
- TARGETED ATTACKS ARE A CYBERCRIME PROBLEM
  - DETERRENCE REQUIRES ENFORCEMENT AND PROSECUTION (GOOD LUCK ON THAT!)
  - IN ABSENCE OF THOSE, PREVENTION IS BEST RECOURSE

PREVENTION IS HARD

- BECAUSE THE SECURITY INDUSTRY ISN'T MAKING THE RIGHT PRODUCTS OR TOOLS
  - NO ONE BOUGHT THE EFFECTIVE ONES BECAUSE THEY DIDN'T UNDERSTAND THEM OR COULDN'T JUSTIFY THEM
- VULNERABILITY AND EXPLOITABILITY ANALYSIS IS CONFUSING
  - WHAT MITIGATIONS ARE ENABLED IN THIS APPLICATION?
  - ARE THEY EFFECTIVE? HAVE THEY BEEN DISABLED?

EXPLOITS SHOULD BE HARD

- AND THEY ARE GETTING HARDER, BUT NOT HARD ENOUGH
- MASS MALWARE INCREASINGLY TURNING TO SOCIAL ENGINEERING TACTICS INSTEAD (I.E. ROGUE AV)
  - MISANTHROPINGLY EFFECTIVE
  - REAL ANTI-VIRUS CAN HANDLE THIS PROBLEM
- DEFENDING AGAINST ADVANCED ATTACKERS REQUIRES ADVANCED DEFENSE SYSTEMS

EAT THE RICH AV VENDORS

- OVERHEARD OUTSIDE RSA EXHIBITION HALL:
  - "VENDOR SPENT $500K ON THEIR BOOTH EXHIBIT AND IT COSTS THEM $90K TO TRANSPORT AND SET IT UP ANYWHERE"
  - THEY HAVE TOO MUCH MONEY FOR NOT SOLVING TODAY'S REAL-WORLD PROBLEMS
- WHY PAY PROTECTION MONEY TO THE MAFIA WHEN YOU ARE STILL GETTING ROBBED EVERY DAY?

STOP CALLING THEM BUFFER OVERFLOWS!

UNLESS A BUFFER IS ACTUALLY BEING OVERFLOWN
(INCREASINGLY RARE)

VULNERABILITY TERMINOLOGY

- BUFFER OVERFLOW
  - WHAT ABOUT OUT-OF-BOUNDS ARRAY INDEXES?
- ARBITRARY CODE EXECUTION
  - WHAT ABOUT SOLARIS TELNETD BUG => AUTH BYPASS
- MEMORY CORRUPTION
  - WHAT ABOUT USE-AFTER-FREE?
  - WHAT ABOUT MEMORY DISCLOSURE VULNERABILITIES?

TYPE SAFETY

- ALL OF THESE VULNERABILITIES ARE FAILURES OF TYPE SAFETY
- C/C++ ARE NOT MEMORY-SAFE OR TYPE-SAFE
- TYPE-SAFE LANGUAGES ONLY HAVE THESE PROBLEMS WHEN THEIR IMPLEMENTATIONS, WRITTEN IN UNSAFE LANGUAGES, HAVE THESE VULNERABILITIES
  - OR PROGRAMS USE "UNSAFE" EXTENSIONS
- WHAT SHOULD WE CALL THESE ISSUES?

"MEMORY TRESPASS"

- "MEMORY TRESPASS VULNERABILITIES ARE SOFTWARE WEAKNESSES THAT ALLOW MEMORY ACCESSES OUTSIDE OF THE SEMANTICS OF THE PROGRAMMING LANGUAGE IN WHICH THE SOFTWARE WAS WRITTEN."
  - DAI ZOVI, "SECURITY APPLICATIONS OF DYNAMIC BINARY TRANSLATION", UNIVERSITY OF NEW MEXICO TECH REPORT TR-CS-2002-38
  - YES, I AM QUOTING MYSELF. DEAL WITH IT.
- CODE INJECTION AND EXECUTION IS ONLY ONE WAY TO EXPLOIT A FEW SPECIFIC CLASSES OF MEMORY TRESPASS VULNERABILITIES

OR...

- ☐ TYPE VIOLATION
- ☐ TYPE SAFETY BYPASS
- ☐ MEMORY SAFETY BYPASS
- ☐ JUST DON'T SAY "BUFFER OVERFLOW" WHEN IT ISN'T
- ☐ DON'T GET ME STARTED ON THE WORD "SHELLCODE"

BUT, BUT, ASLR, DEP!

- ASLR AND DEP DO A GREAT JOB OF MAKING EXPLOITATION OF SERVER-SIDE VULNERABILITIES IMPOSSIBLE IN THE VAST MAJORITY OF CASES
- LOW-INTEGRITY PREVENTS WRITING, BUT NOT READING YOUR SENSITIVE DOCS AND INFORMATION
- SCRIPTABLE CLIENT APPLICATIONS OFFER A MUCH LARGER ELEMENT OF ATTACKER CONTROL
  - YIELDS MORE POSSIBILITIES FOR EVADING ASLR
- CODE-REUSE EXPLOIT TECHNIQUES CAN BE USED TO BYPASS DEP

CODE-REUSE EXPLOITS

- RETURN-TO-LIBC (SOLAR DESIGNER, 1997)
  - RETURN INTO FUNCTIONS IN LIBC
- BORROWED CODE CHUNKS (KRAHMER, 2005)
  - LINK RETURNS TO SINGLE-INSTRUCTIONS
- RETURN-ORIENTED PROGRAMMING (SHACHAM, 2007)
  - TURING COMPLETE W/ COMPILER FOR C-LIKE LANGUAGE

TACTICS VS. STRATEGY

- MALICIOUS INJECTED CODE IS NOT THE TRUE PROBLEM
  - IT IS ONLY THE MOST COMMON EXPLOITATION TACTIC
  - CODE-REUSE EXPLOITATION TECHNIQUES DON'T NEED TO INJECT ANY CODE, WILL REUSE WHAT IS THERE
- THE STRATEGY IS TO MAKE THE TARGET APPLICATION DO UNEXPECTED THINGS IN A WAY USEFUL TO THE ATTACKER
  - UNEXPECTED/UNDESIRABLE BEHAVIOR IS PROBLEM

MY SANDBOX SOAPBOX

- WHY DOES MY BROWSER NEED TO BE ABLE TO WRITE TO ANYWHERE EXCEPT FOR ~/DOWNLOADS?
- WHY DO DOC READERS, IM CLIENTS, NEED TO WRITE FILES AT ALL?
- MULTI-USER DAC SECURITY MODEL IS ILL-SUITED TO THE DESKTOP
- WE NEED A NEW MULTI-APPLICATION DESKTOP SECURITY MODEL
  - PHONES (IPHONE AND ANDROID) ALREADY HAVE THIS
  - IPHONE PREVENTS INJECTED CODE AND APP MISBEHAVIOR

QUESTIONS?

@DINODAIZOVI / DDZ@THETA44.ORG