COMSEC Consulting

The art of securing your business

OWASP Top Ten Backdoors

Yaniv Simsolo, COMSEC Consulting

“ The news about the above agreement was posted on Cisco site in mid 1998. Shortly this news was removed from Cisco website. Gradually all this information which was readily available about backdoors and doorbells was removed from the internet.”

OWASP Top Ten Backdoors

- Prologue
- Definition
- Top Ten Most Common Backdoors
- Impacts
- Summary

OWASP Top Ten Backdoors

- The OWASP Top Ten Backdoors paper provides a list of the most common backdoors in applications.
- Just like the OWASP Top Ten outlines the top ten mistakes developers make in applications, the top ten backdoors discuss the top ten features in systems that leave the application vulnerable.
- The Top Ten Backdoors are relevant to any application including web applications, client-server applications, multi-tier enterprise applications etc.

Prologue

- Backdoors are more common then developers and system professionals think.
- Hackers and malicious users can exploit backdoors easily, without leaving any special traces in the system.
- For example, a common unconventional backdoor in enterprises is a middle-tier system that does not employ authentication and authorization mechanisms
  - “Trust-based architecture”
  - Any user within the enterprise can exploit such a backdoor easily by requesting the middle-tier system for confidential data and un-authorized actions within the enterprise systems.

Definition

- Definitions of backdoor:
  - A hidden entrance to a computer system that can be used to bypass security policies (MS definition).
  - An undocumented way to get access to a computer system or the data it contains.
  - A way of getting into a guarded system without using the required password.

Definition

- Problem: definitions are too wide
- Fine separation line between security vulnerabilities and backdoors.
- Backdoor is:
  - A security vulnerability
  - That can be used to bypass security policies and mechanisms in a system
- Two main types of backdoors:
  - Conventional (hidden parameters, redundant interfaces, etc.)
  - Unconventional
- Considering relative risk, exposure and damage – the unconventional backdoors are more dangerous

Top Ten backdoors

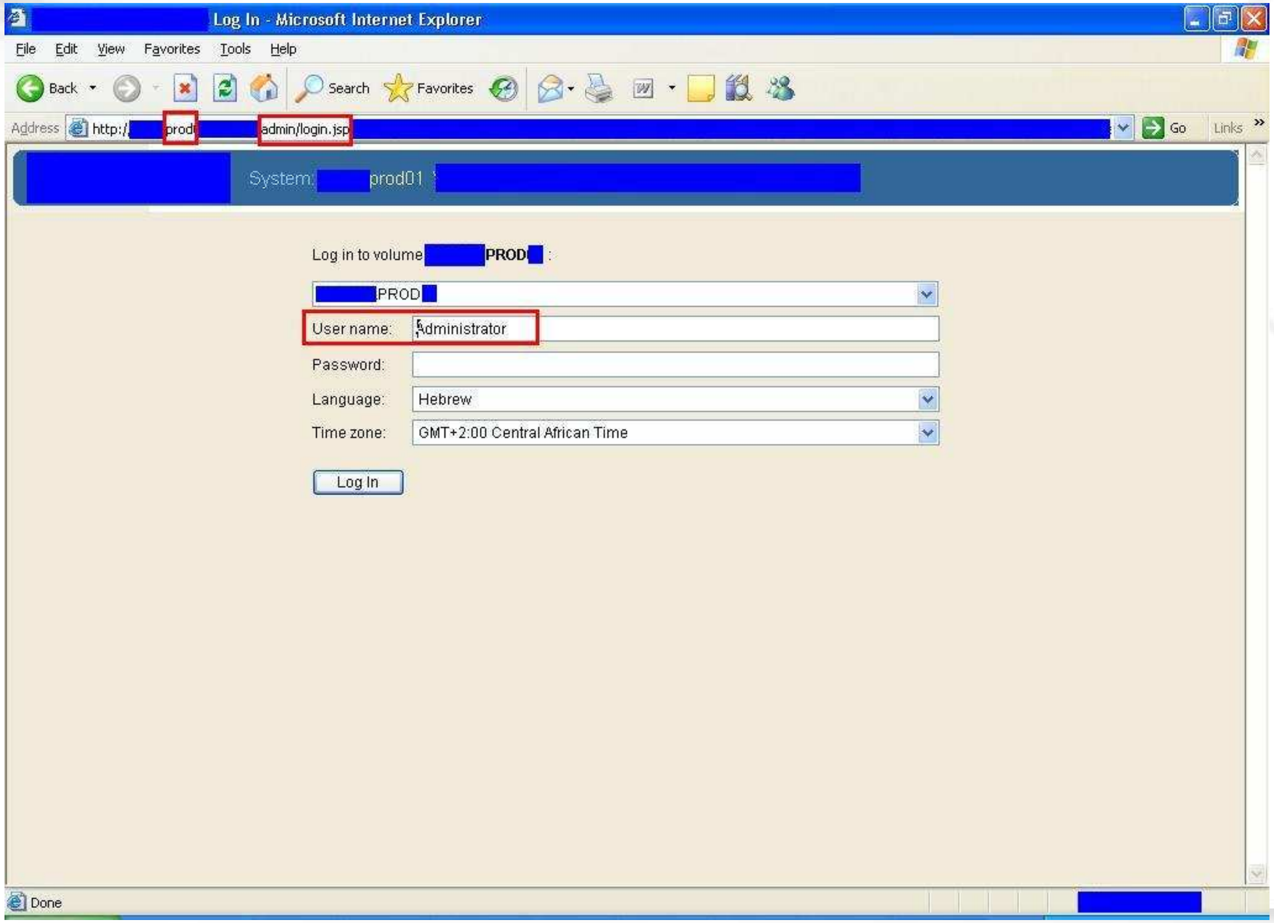
Conventional backdoors

OWASP Top Ten Backdoors, Number 1

- **Administration And Management Interfaces Exposed**
  - */admin - everywhere
  - Access control management - limited scope
  - Only protected by authentication. Usually only PWD protection.
  - Administration interfaces are thus exposed to:
    - Brute-Force
    - Dictionary attacks
    - Lockout attacks (depending on architecture)

OWASP Top Ten Backdoors, Number 1

- **Administration And Management Interfaces Exposed**



[redacted] Log In - Microsoft Internet Explorer

http://[redacted]prod[redacted]admin/login.jsp[redacted]

System: [redacted] prod01 [redacted]

[redacted]

Log in to volume [redacted]PROD[redacted] :

[redacted]PROD[redacted]

User name: Administrator

Password:

Language: Hebrew

Time zone: GMT+2:00 Central African Time

Log In

Done [redacted]

OWASP Top Ten Backdoors, Number 1

- **Administration And Management Interfaces Exposed**
  - Allowing anyone to take control over the application
  - 3rd party systems force backdoors on organizations
  - Once the administrator credentials are default – hackers heaven!
  - OWASP A10 – Insecure Configuration Management

OWASP Top Ten Backdoors, Number 2

- **Redundant interfaces/functions/features**
  - debug=TRUE
  - Backdoors by design
  - Uploaded to production environment
    - By mistake
    - On purpose
    - Due to faulted procedures
  - Enable various actions and control over systems
  - Exploitable at large by hackers
  - OWASP A10 – Insecure Configuration Management
  - OWASP A1 – Unvalidated Input

OWASP Top Ten Backdoors, Number 3

- **Hidden parameters**
  - *=-999
  - Backdoors by design
  - Uploaded to production environment on purpose
  - 3rd party systems expose the enterprise:
    - Without protection
    - Without knowledge of backdoor existence
  - Enable various actions and control over systems
  - Exploitable at large by hackers
  - OWASP A1 – Unvalidated Input?

OWASP Top Ten Backdoors, Number 4

- **Redundant users**
  - guest, testuser, scott (tiger)
  - Usually default users
  - Uploaded to production environment due to faulted procedures
  - Common knowledge
  - May enable hackers to take total control over the system
  - Easily mitigated
  - OWASP A10 – Insecure Configuration Management

OWASP Top Ten Backdoors, Number 5

- **Authorization for 3rd party access**
  - Backdoors by design
  - Uploaded to production environment
    - By design
    - By mistake
  - Apparently difficult to control authorization issues
  - 3rd party access may expose the enterprise or system without protection
  - Should be controlled by procedures
  - Organization awareness and continuous monitoring – a must
  - OWASP A10 – Insecure Configuration Management

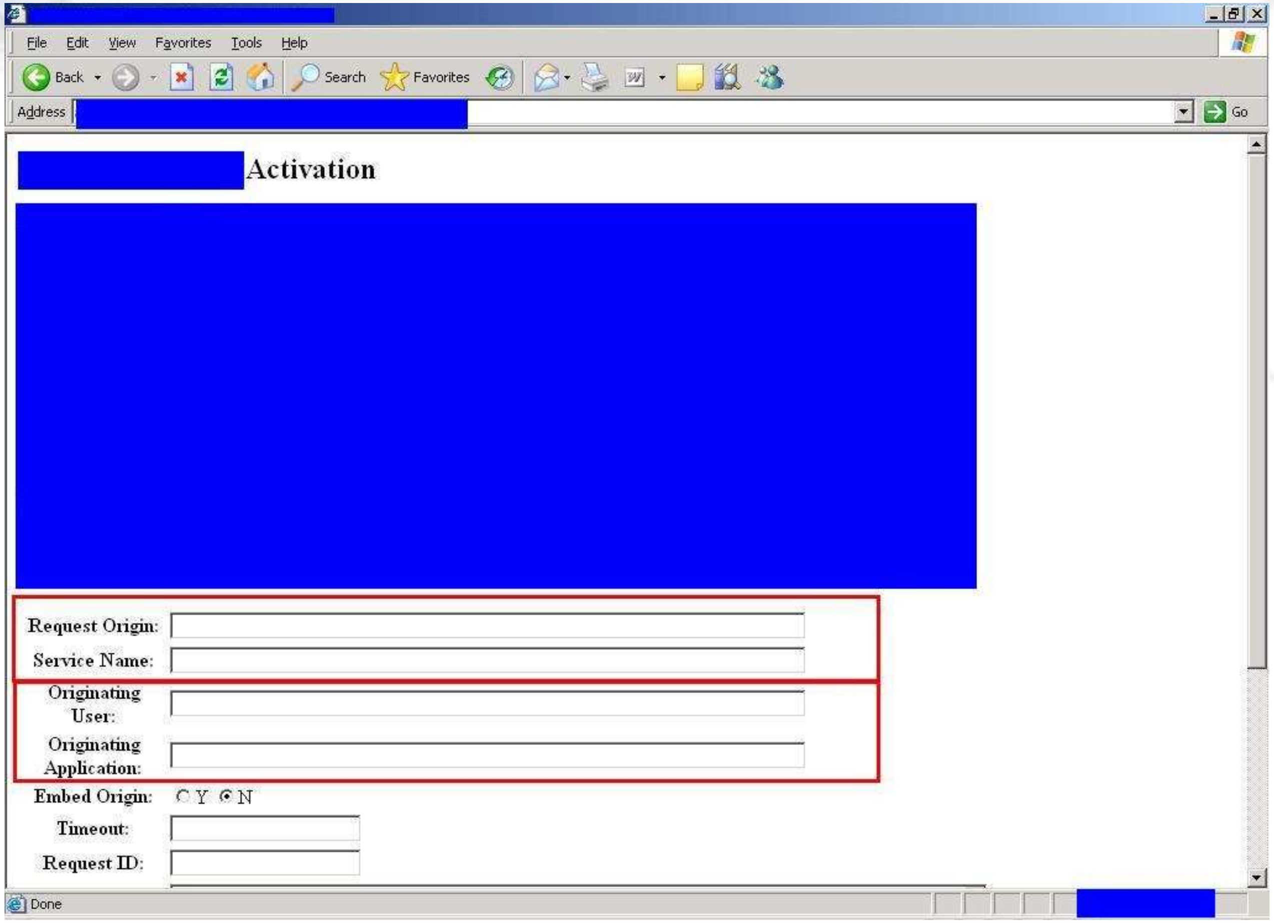
Unconventional backdoors

OWASP Top Ten Backdoors, Number 6

- **Authentication and Authorization between application components**
  - Most common application level backdoor vulnerability
  - Difficult to Fix.
    - In 3rd party systems – sometimes impossible to fix
  - Leaves the system totally open to the knowledgeable hacker

OWASP Top Ten Backdoors, Number 6

- Middle-tier system – actual API in production environment -
  No authorization, No Authentication



[redacted] Activation

[redacted]

Request Origin:

Service Name:

Originating User:

Originating Application:

Embed Origin: ○ Y ● N

Timeout:

Request ID:

OWASP Top Ten Backdoors, Number 6

- **Authentication and Authorization between application components**
  - Once open to the web – security disaster
  - Within the enterprise:
    - Common knowledge for developers and others
    - Embedded in systems’ design
    - Suggests flawed development procedures
  - Once exposes other enterprise systems - security nightmare
  - OWASP A3 – Broken Authentication
  - OWASP A10 – Insecure Configuration Management

OWASP Top Ten Backdoors, Number 7

- **Old Users in Systems**
  - Probably most common in enterprises
  - Originally created according to standard procedures
  - Old users are
    - backdoors to systems
    - enabling identity fraud
    - bypassing systems’ security mechanisms
    - very difficult to locate in real time
  - Hard to locate, remove, and control

OWASP Top Ten Backdoors, Number 7

- **Old Users in Systems**
  - Commonly exploited by employees for various purposes (not necessarily innocent)
  - Commonly exploited by developers as “standard” development process
  - Old users that were administrators enable ANYONE in becoming an administrator of the system.
    - In an enterprise core system – jackpot for malicious users.
  - All the above – discovered on daily basis in organizations.
  - OWASP A10 – Insecure Configuration Management

OWASP Top Ten Backdoors, Number 8

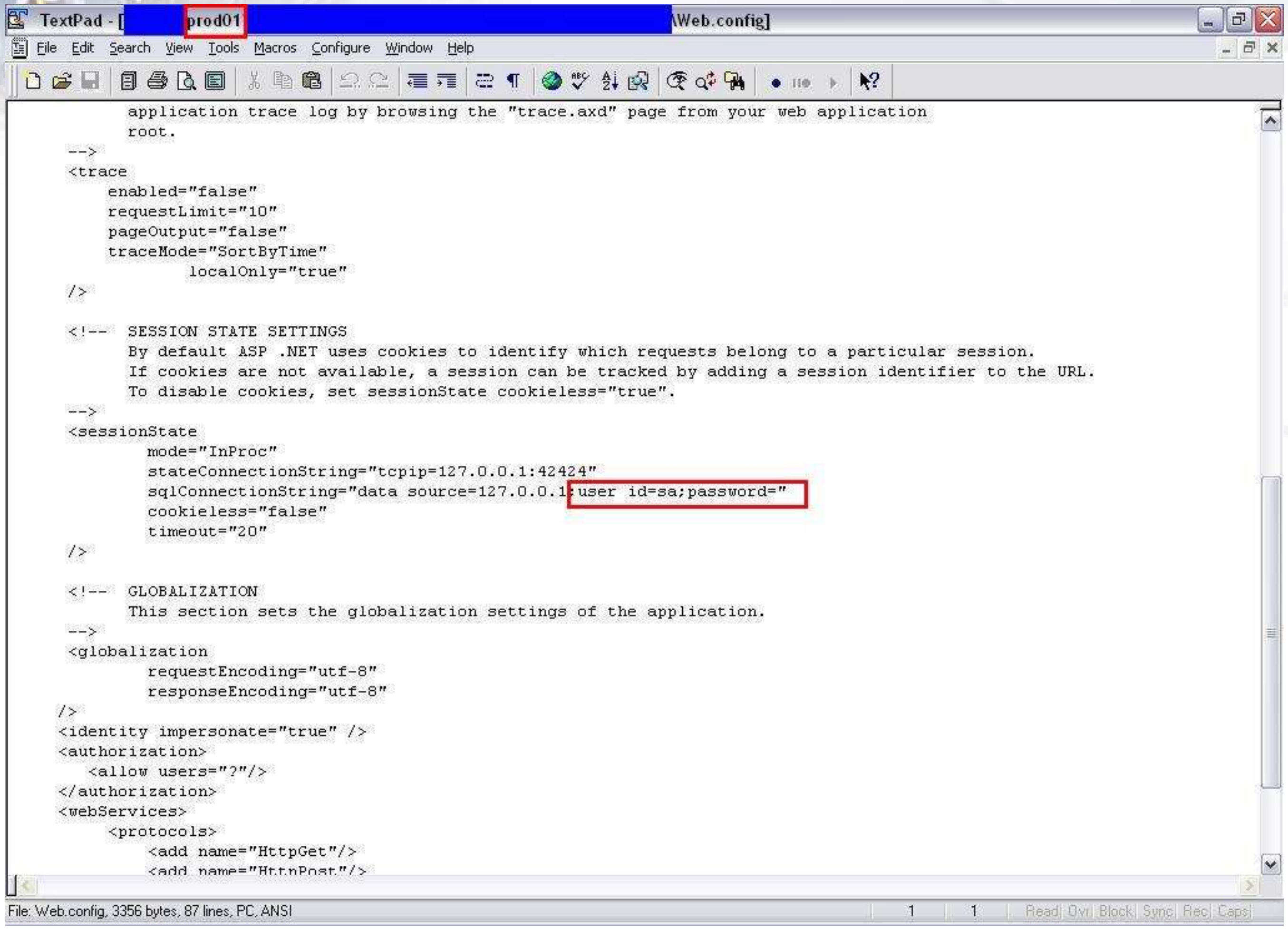
- **Flawed hardening**
  - xp_cmdshell
  - Perfect hardening is difficult to achieve
  - Hardening of ALL system components is mandatory
  - Common failure in organizations – lack of hardening
  - Enables malicious entities multiple attack vectors, up to a total control of the system
  - OWASP A10 – Insecure Configuration Management

OWASP Top Ten Backdoors, Number 8

- **Flawed hardening**
  - Most (aware) organizations perform:
    - OS hardening
    - Application servers hardening
    - DB hardening
  - What about application hardening?
  - OWASP A10 – Insecure Configuration Management

OWASP Top Ten Backdoors, Number 8

- **Flawed hardening**


TextPad - [[redacted]prod01[redacted]\Web.config]
File Edit Search View Tools Macros Configure Window Help

```
       application trace log by browsing the "trace.axd" page from your web application
       root.
 -->
 <trace
     enabled="false"
     requestLimit="10"
     pageOutput="false"
     traceMode="SortByTime"
             localOnly="true"
 />

 <!--  SESSION STATE SETTINGS
       By default ASP .NET uses cookies to identify which requests belong to a particular session.
       If cookies are not available, a session can be tracked by adding a session identifier to the URL.
       To disable cookies, set sessionState cookieless="true".
 -->
 <sessionState
         mode="InProc"
         stateConnectionString="tcpip=127.0.0.1:42424"
         sqlConnectionString="data source=127.0.0.1;user id=sa;password="
         cookieless="false"
         timeout="20"
 />

 <!--  GLOBALIZATION
       This section sets the globalization settings of the application.
 -->
 <globalization
         requestEncoding="utf-8"
         responseEncoding="utf-8"
/>
<identity impersonate="true" />
<authorization>
   <allow users="?"/>
</authorization>
<webServices>
     <protocols>
         <add name="HttpGet"/>
         <add name="HttpPost"/>
```

File: Web.config, 3356 bytes, 87 lines, PC, ANSI   1   1   Read Ovr Block Sync Rec Caps

OWASP Top Ten Backdoors, Number 9

- **Exposed Configuration Data**
  - Common within organizations
  - Linked databases
  - PWD files
  - Difficult to mitigate
    - Weaved into systems’ architecture
    - Collateral implications on the enterprise
    - Even encryption is difficult
  - May effect other systems

OWASP Top Ten Backdoors, Number 10

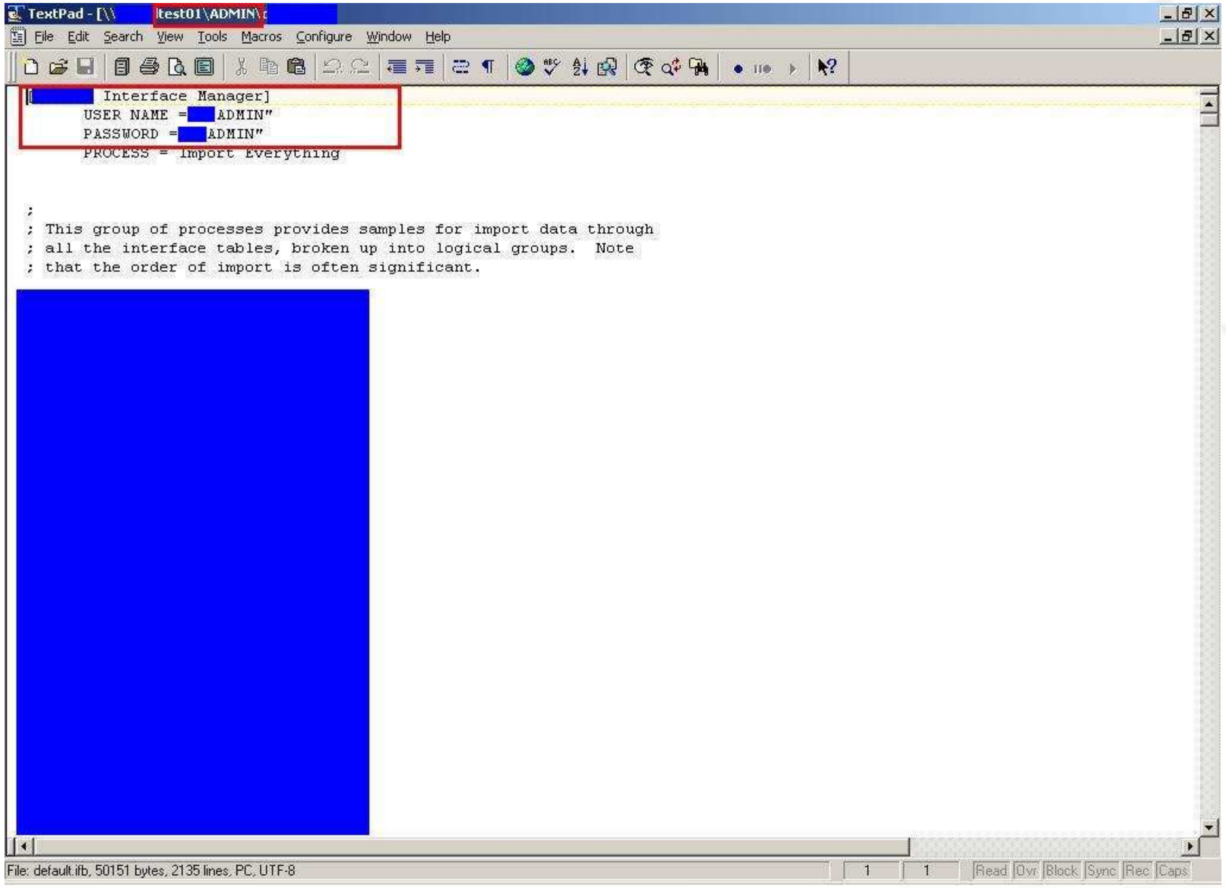
- **Lack of separation between environments**
  - Not a backdoor in itself
  - However:
    - A security vulnerability
    - That can be used to bypass security policies and mechanisms in a system
  - A problem for most organizations and enterprises

OWASP Top Ten Backdoors, Number 10

- **Lack of separation between environments**
  - Only two options for mitigation:
    - Obfuscate data in test and development environments
    - Employ identical security mechanisms and policies in production and other environments
  - Both very difficult to employ

OWASP Top Ten Backdoors, Number 10

- **Identical authentication parameters in PROD and TEST environments**


TextPad - [\\ [redacted] test01\ADMIN\c [redacted]
File Edit Search View Tools Macros Configure Window Help

```
[ [redacted] Interface Manager]
      USER NAME = [redacted] ADMIN"
      PASSWORD = [redacted] ADMIN"
      PROCESS = Import Everything


;
; This group of processes provides samples for import data through
; all the interface tables, broken up into logical groups.  Note
; that the order of import is often significant.
[redacted]
```

File: default.ifb, 50151 bytes, 2135 lines, PC, UTF-8 1 1

Read Ovr Block Sync Rec Caps

Impacts

Impacts

- Backdoors can not be mitigated easily
- Are deeply established within the enterprise
- Mitigation is resource-consuming
- Usually represented as vulnerabilities:
  - Hiding the full impact
  - Lacking total resolution
  - Limited scope of referencing (a backdoor in system can affect other systems)

Impacts

- Impacts are larger then conceived
- Some backdoors may even enable creating additional backdoors
- Furthermore – impacts may effect multiple systems
  - (Note to self: “watch security managers responses for such backdoors discovery” ☺)

Summary

- Backdoors are abundant
- Represent a security nightmare
- Like most application level vulnerabilities - best if discovered and mitigated in design and development phases
- Should not be ignored

Questions?