

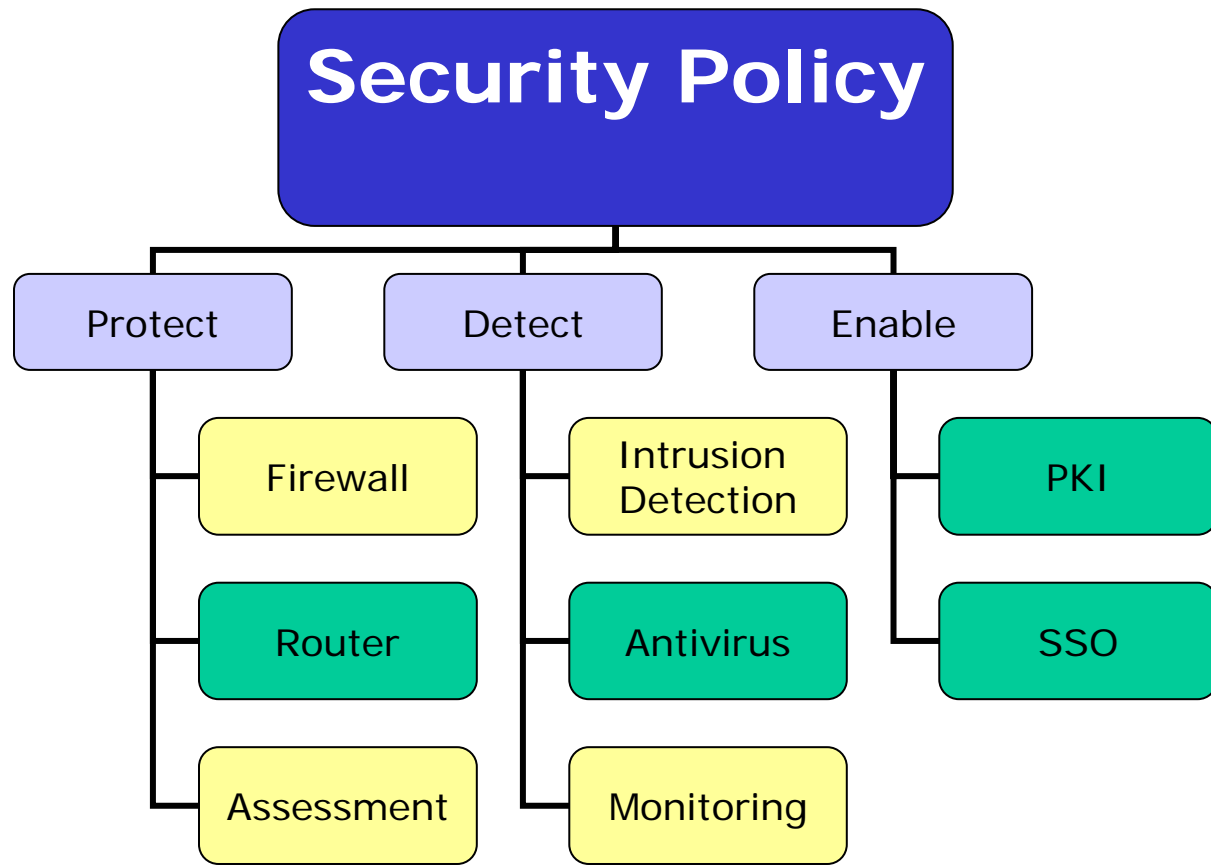
Intrusion Trend 2001-2005 & Survivable Systems

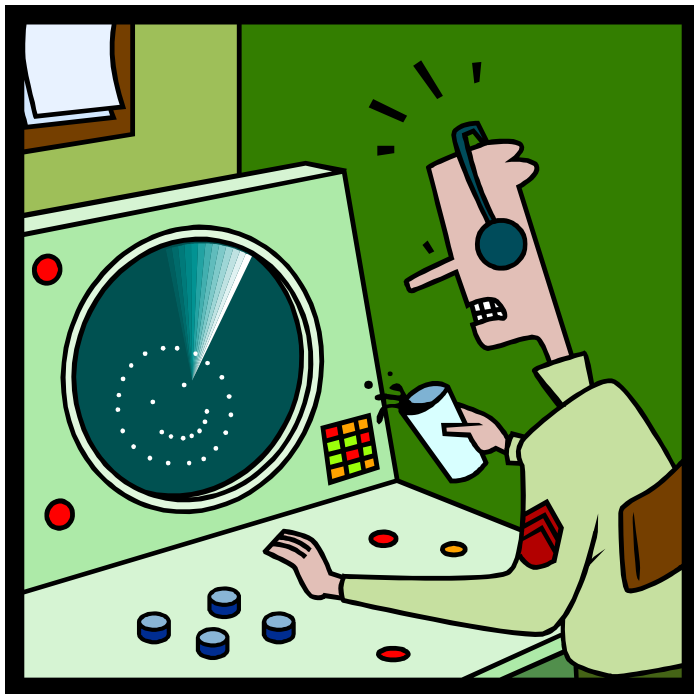
Norman PAN

Doctor A Security Systems (HK) Ltd.

8 May 2002

- Who are we?
- What to expect?
 - Recent Intrusion example
 - Intrusion Trend
 - ❖ CERT/CC
 - ❖ Our live data
 - Survivable Systems
 - ❖ CERT/CC





IDnA

■ Detection

- 7x24 Security Monitoring
 - ❖ Intrusion Detection
 - ❖ Web Integrity

■ Defense (in-depth)

- Firewall
- Web Security

■ Assessment

Before we start

Microsoft IIS

... um ... again?....

<http://www.microsoft.com/technet/security/bulletin/MS02-018.asp>

What is the most likely cause to this web defacement?

- a) The victim does not have a packet filter firewall.
- b) The victim web server is not patched.
- c) The victim does not have a Network Intrusion Detection installed.
- d) The attacker is a genius, he can hack into any web site.

.. = go up one directory

%25 = %

%5c = \

http://192.168.1.39/scripts/..%255c..
%255c..%255cwinnt\system32\cmd.
exe?/c+dir+c:

? = parameter following

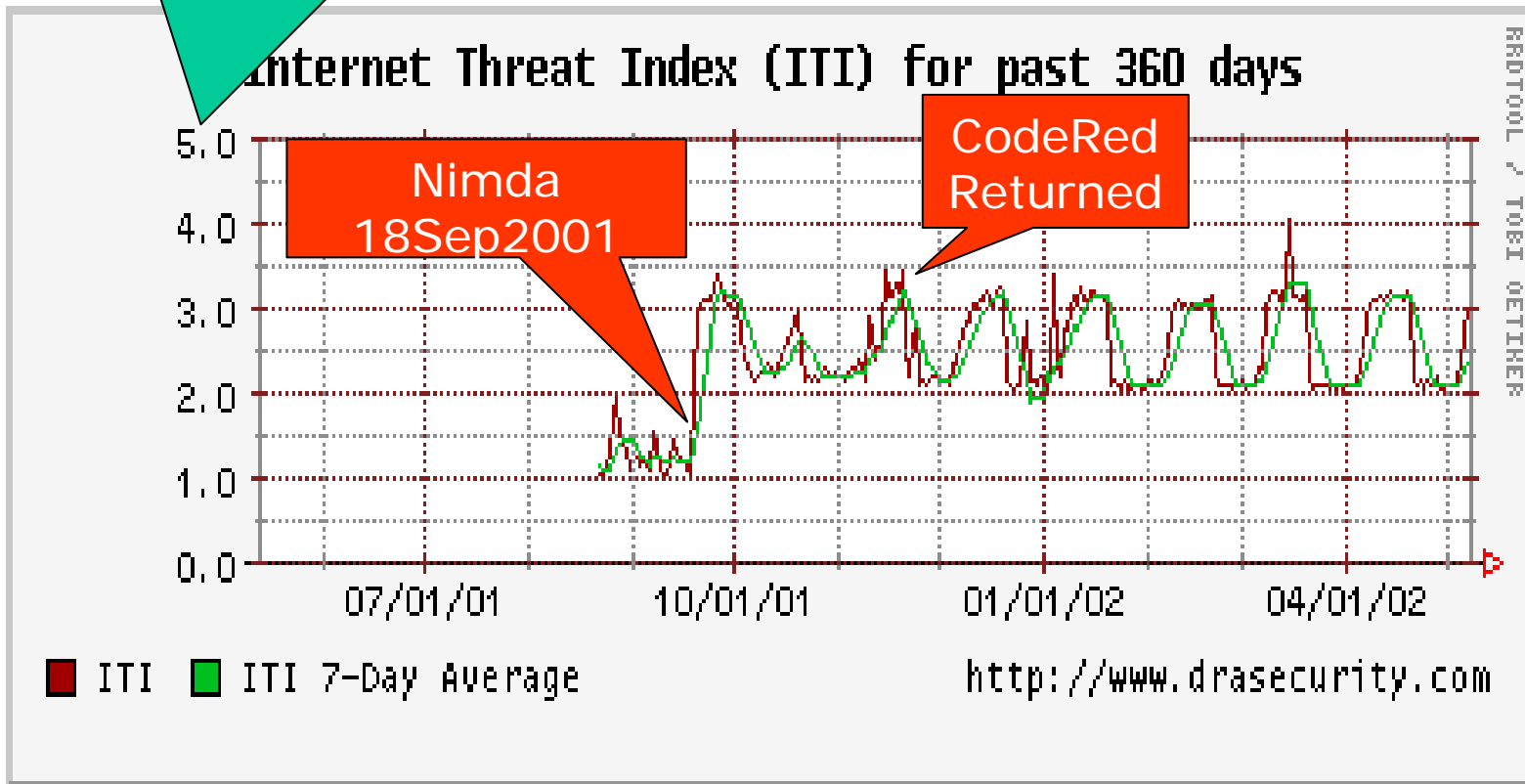
/c = this is a 1 line command

+ = space

http://192.168.1.39/scripts/..\..\..\win
nt\system32\cmd.exe?/c+dir+c:

Intrusion Trend 2001-2005

Unpatched Systems Will be compromised by # of SAN Top 10 vulnerabilities



http://www.drasecurity.com/index_trend.html

Previously

- Widespread scanning since 1997
- Vulnerabilities exploited after scanning complete
- A person to initiate additional attack
- Target one by one

Today

- More advanced scanning patterns
- Exploit vulnerabilities as a part of the scanning
- Self initiate new attack cycles
 - (e.g. CR/Nimda global saturation in 18 hours)
- Able to manage and coordinate large number of deployed attack tools across the Internet

Previously

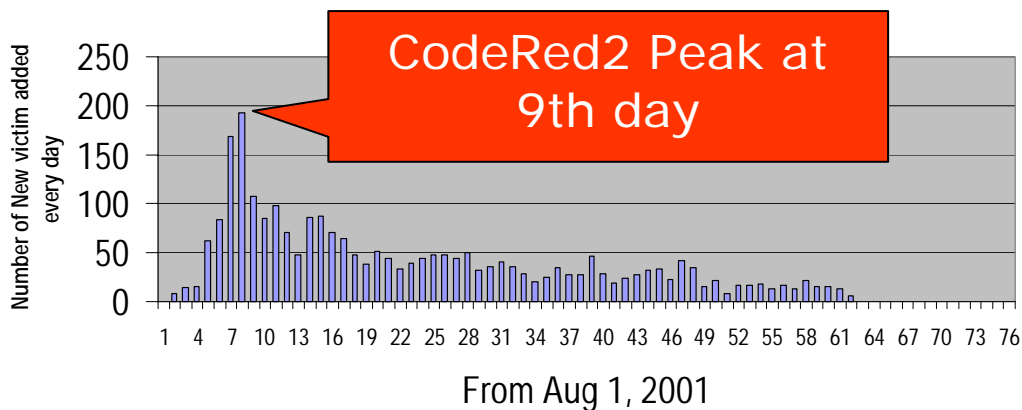
- Static, signature was easy to identify
- Single defined sequence
- One type of attack at a time

Today

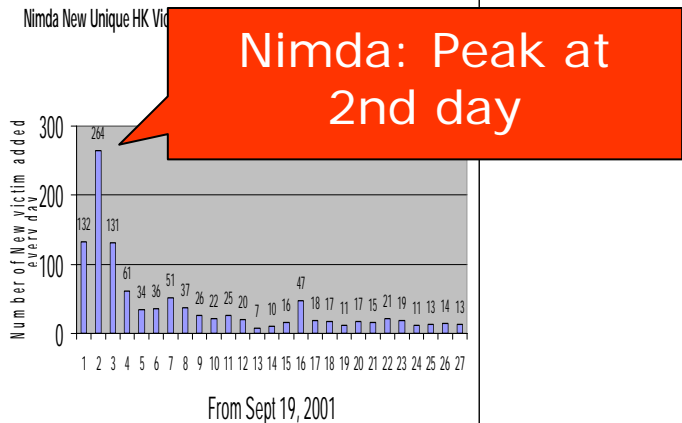
- Anti-forensic
 - Obfuscate technique
 - More difficult to analyze
- Dynamic
 - Vary patterns and behaviors in random, predefined or even managed.
- Modular
 - Portions of the tools can be changed, upgraded or replaced
 - Polymorphic

- Number of newly discovered vulnerabilities DOUBLE each year.
- Automated discovery of new vulnerabilities => “Time to patch” increasingly small

Code Red Worm 2 New Unique HK Victim IP addresses detected by Doctor A Security Systems (HK) Ltd.



Nimda New Unique HK Victim



- Designed to bypass firewall configuration
 - IPP (Internet Printing Protocol)
 - WebDav (Web-based Distributed Authoring and Versioning)
 - “Firewall Friendly” => Firewall bypass
 - Mobile code (ActiveX controls, Java and Javascript) => Vulnerable systems ^ difficult to protect.

- Security on the Internet,
 - highly Interdependent.
 - Each System's exposure \leq Security of the rest of the Internet
- ^ Easy to deploy a devastating attacks against a single victim
 - ^ Automation of deployment
 - ^ Sophistication of attack tool management
- ^ Asymmetric nature of the threat

Attack 1 – DDOS

- Distributed Denial of Service
- Single attacker to install tools and control 100,000 compromised system to attack one or more victim
- Attackers are actively searching address blocks with high concentrations of vulnerable systems with high speed connections
 - Universities
 - Cable modem, DSL ...

Attack 2 – Worms

- Virus: requires a user to do something to continue the propagation.
- Worm: Self propagating malicious code.
 - Code Red infected 250,000 system in 9 hours on 19 July 2001
 - DOS attack: Code Red (or generic worm propagation effectiveness)
 - Web defacement: Sadmin/IIS, Code Red
- Economic Impact (Computer Economics' estimation):
 - Code Red: US\$2.6 billion
 - Sircam: US\$1.3billion
 - 911: US\$15.8billion to restore IT and communication capabilities.

Attack 3 – Attacks on DNS

- Cache poisoning
 - Cache bogus information, redirect to attacker's intended site.
- Compromised data
 - 20% of TLD domains are vulnerable
 - 70% are "status unknown"
- Denial of Service
 - What if .com TLD was too busy => effective outage
- Domain Hijack
 - Insecure mechanism of updating domain registration, attacker take control of legitimate domains.

- Attack 4 – Attacks against or using routers
 - Routers as attacking platform
 - ❖ If the router's password is password
 - Denial of Service
 - ❖ Attack the router
 - ❖ Router is designed to pass traffic (Sorting mail < > Reading mail)
 - Exploitation of trust relationship between routers

To Auditors

Are the systems under attack?

This is NOT the Right question.

**Can the system SURVIVE
under attack?**

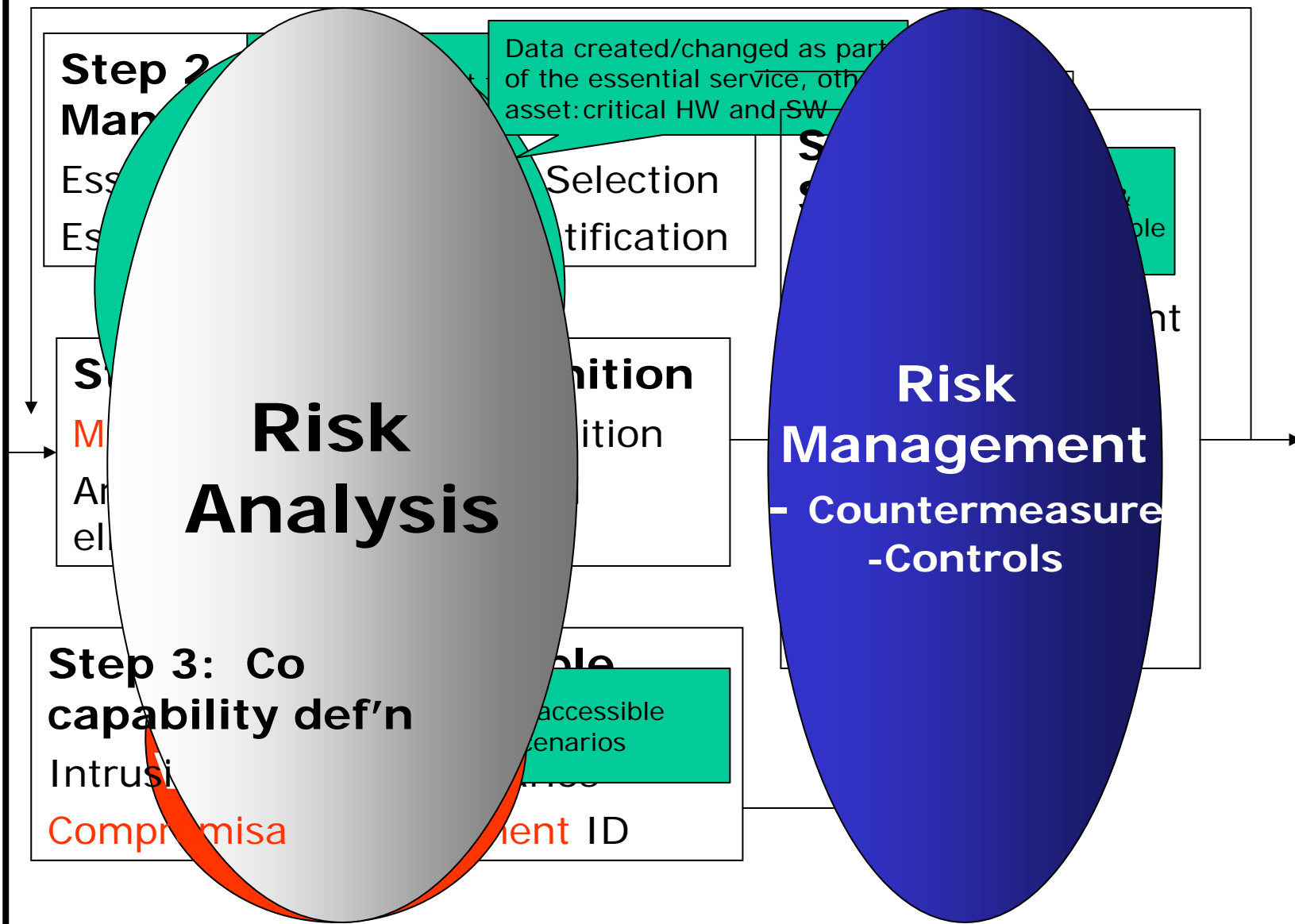
Survivability

- is the capability of a system to fulfill its mission,
- in a timely manner
- in the presence of attacks, failures, or accidents

Survivability

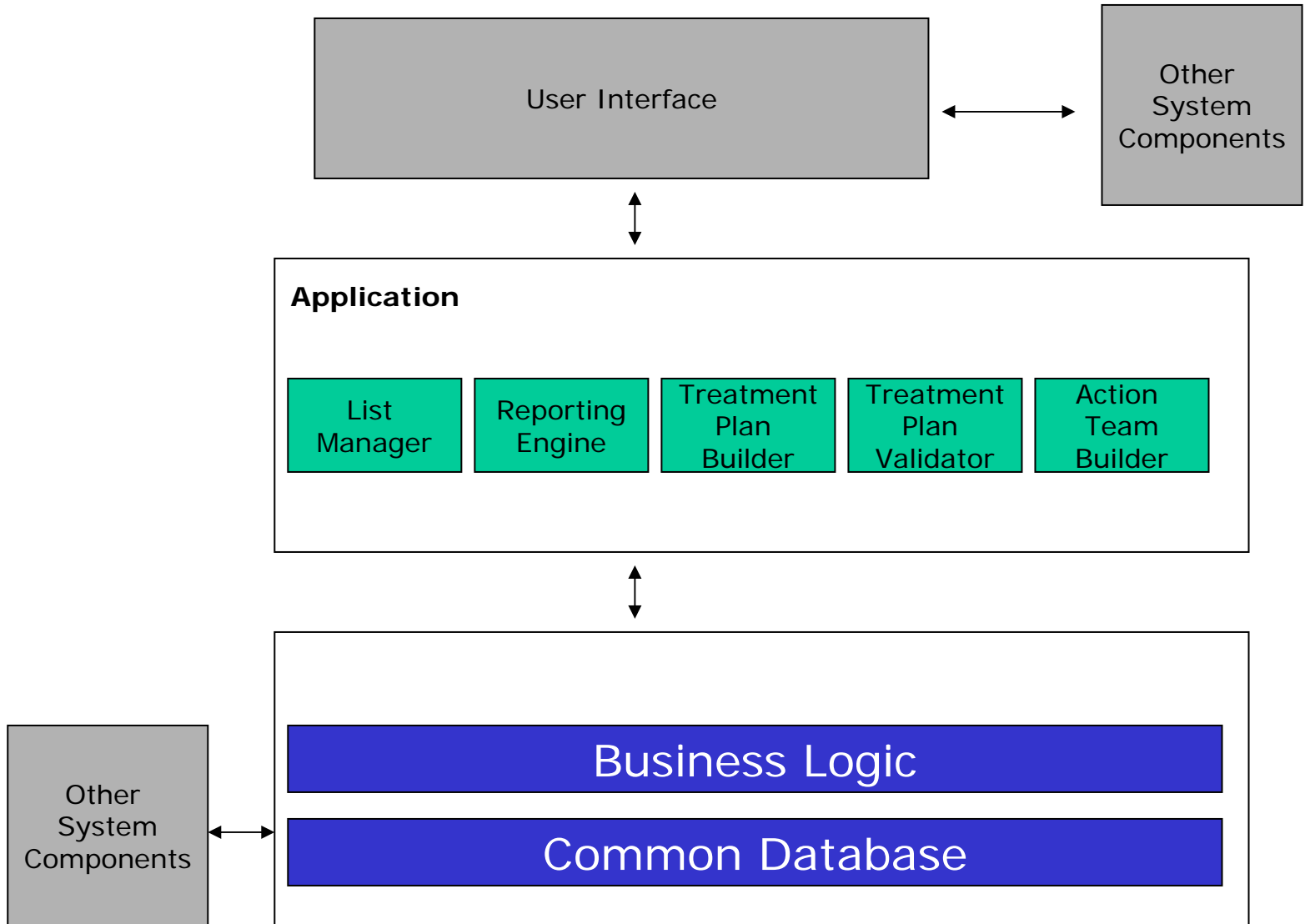
- requires capabilities for Intrusion
 - **R**esistance
 - **R**ecognition
 - **R**ecovery

Doctor A Security



Case 1

A Hospital application



Intrusion Scenario

Unauthorized User modify or view TP by spoofing a legitimate user

Softspot

Treatment Plans

Resistance Strategy

Current:

None, No timeout.

Recommended:

Add a short logout timer for terminals {1}

Recognition Strategy

Current:

None, Except for unusual number of denied TP access.

Recommended:

Add logging, access control, and illegal access thresholds {1}

Recovery Strategy

Current:

Get list of modified TP thru spoofed user transaction history, manual recovery.

Recommended:

Develop a recovery procedure and support it in the UI {1}

Intrusion Scenario

Unauthorized User corrupts the DB leading to loss of trust in all validated TPs

Softspot

Treatment Plans

Resistance Strategy

Current:
Security model in DB protects TP vs corruption.

Recommended:

Implement live replicated DBs that cross check for validity {5}

Recognition Strategy

Current:
None, Except when a provider happens to recognize a corrupt TP.

Recommended:

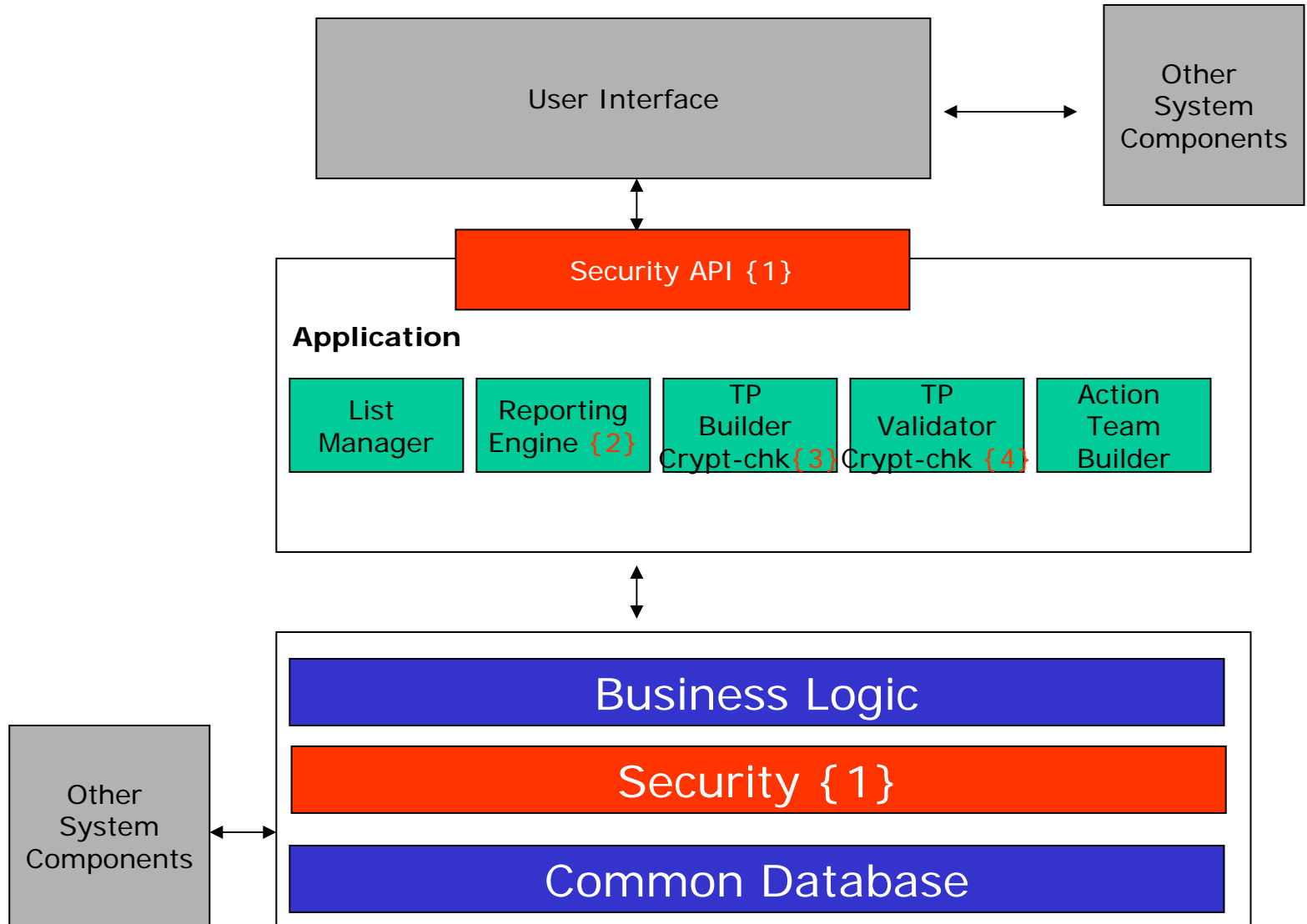
Add and check crypt-checksums on TPs in DB {3,4}

Recovery Strategy

Current:
Locate an uncorrupted backup or reconstruct TPs from scratch

Recommended:

Reduce the backup cycle to quickly rebuild once a corrupt DB is detected {5}



Q & A