The Cyber Plaque: Myth or Reality

Sean Lim, Vice President – EC-Council

Pentagon trains workers to hack Defense computers

By **Larry Shaughnessy**, CNN Pentagon Producer
March 11, 2010 -- Updated 0027 GMT (0827 HKT)

The idea behind the Pentagon's training is that thinking like a hacker can beat a hacker.

STORY HIGHLIGHTS

Washington (CNN) -- The Pentagon is training people to hack into its own computer networks.

"To beat a hacker, you need to think like one," said Jay Bavisi, co-founder and president of the International Council of Electronic Commerce Consultants, or EC-Council. His company was chosen by the Pentagon to oversee training of Department of Defense employees who work in computer security-related jobs and certify them when the training is complete.

EC-Council Courseware certified to have met the CNSS Standards by the United States National Security Agency (NSA) and the Committee on National Security Systems (CNSS)

EC-Council Certified Ethical Hacker (C|EH), Computer Hacking Forensics Investigator (C|HFI), Disaster Recovery Professional (E|DRP), Certified Security Analyst (E|CSA) and Licensed Penetration Tester (L|PT) Courseware has been certified at the highest national level by National Security Systems (CNSS). The CNSS is a federal government entity under the U.S. Department of Defense that provides procedures and guidance for the protection of national security systems. The NSA certified these programs as meeting the 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals in the federal government.

http://www.eccouncil.org

EC-Council

Certified Ethical Hacker Program Achieves DoD 8570

C|EH™ Certified Ethical Hacker

The Certified Ethical Hacker (CEH) program is a recognized certification for the United States Department of Defense's (DoD) computer network defense Service Providers (CND-SP's), a specialized personnel classification within the DoD's information assurance workforce.

This recognition falls under the auspices of DoD Directive 8570 Information Assurance Workforce Improvement Program. Directive 8570 provides clear guidance to information assurance training, certification and workforce management across all affected components of the DoD.

Unravel the Enigma of Insecurity

DEPARTMENT OF DEFENSE (DoD 8570.1) ENDORSED

"The course was very informative and provided a sound base upon which to build many other certifications and skills. I will personally be recommending that this course be mandatory for all personnel within our cyber threat section.

- DoD Participant

Texas State Technical College

Northwest Vista College

UNIVERSITY OF PITTSBURGH

HOLYOKE COMMUNITY COLLEGE
Futures Inspired
HOLYOKE CC

OHIO NORTHERN UNIVERSITY

UNIVERSITY OF TEXAS

HILL COLLEGE

AMERICAN CAREER UNI

GEORGE MASON UNIV - PRINCE WILLIAM

TRUMBULL CAREER TECH CTR

MARYMOUNT UNIVERSITY

UNIVERSITY OF CENTRAL OKLAHOMA

SOUTH PLAINS COLLEGE LUB

VATTEROTT COLLEGE

COLLINS COLLEG

ITT ONLINE SCHOOL

J SARGEANT REYNOLDS CC - PARHA RD

HOWARD COLLEGE

ROWAN CABARRUS COMMUNITY COLLEGE

CLOVER PARK TECH C

ACADEMY OF COURT REPORTING & TECHNOLOGY

ODESSA COLLEGE

DELTA COLLEGE

AMERICAN INTERCONTINENTAL UNVIVERSITY

LAKE LAND COLLEGE

PASCO-HERNANDO COM COLLEGE

MILLER-MOTTE TECH COLLEGE

KAPLAN UNIVERSITY

SOLANO COLLEGE

NORTH SCHUYLKILL SCHOOL DIST

SOUTHERN POLYTECHNIC STATE UNIVERSITY

ASHTABULA CNTY TECH CAREER CENTE

HILL JUNIOR COLLEGE

MCCANN SCHOOL OF BUSINESS

CARL ALBERT STATE COLLEGE

EDGECOMB COMMUNITY COLLEGE

NAPA VALLEY COLLEGE

SOUTHWESTERN COMMUNITY COLLEGE

BLOOMSBURG AREA HIGH SCHOOL

DONA ANA COMMUNITY

WESTERN GOVERNORS UNIVERSITY

GLENDALE COMMUNITY COLLEGE
GLENDALE CC

Leeds City College - Network Academy, United Kingdom

Bournemouth University, UK/Europe

CFA-AFTI, France

Northumbria University, UK/Europe

REGENT UNIVERSITY

PINELLAS TECH ED

Budapest University of Technology and Economics, Hungary

ESAIP, France

ROC Midden Nederland, Netherlands

HILLSBOROUGH COMMUNITY COLLEGE - DALE MABRY

LOS ANGELES SOUTHWEST COLLEGE

Staffordshire University, United Kingdom

ACISSI Maubeuge

Africa

EASTERN KENTUCKY UNIVERSITY

MCLENNAN COMMUNITY COLLEGE

Institut Informatique et Entreprise, France

School of Information Systems and Technology, University of KwaZulu-

Puntos clave

- **ECC es una organizacion internacional**
- **Trabaja el rededor del mundo con organizaciones como:**
  - **ONU,**
  - **PENTAGON,**
  - **Departamento de Defensa (USA)**
- **Trabajamos actualmente con diversas universidades en el mundo**

CyberWar – A New Mindset

- **Taxanomy of War vs CyberWar**
- **When did the war start?**
- **Who are the opponents?**
- **What key targets are they after?**
- **When has the war ended?**
- **What was the damage?**
- **Geneva War Convention – protocols of war**

Experts: US Is Not Prepared to Handle Cyber Attacks

In Congressional testimony, authorities on cyber defense say neither government agencies nor private companies are ready for what may come

By Tim Wilson
Site Editor, *Dark Reading*

If the bad guys launched a coordinated cyber attack on the United States tomorrow, neither government nor industry would be able to stop it, experts warned legislators yesterday.

At a hearing held by the House Permanent Select Committee on Intelligence, cyber defense experts testified that government agencies are insufficiently coordinated to handle an attack, and that efforts to build a defense have not adequately addressed issues in the private sector.

"The Department of Homeland Security lacks the personnel, capability, authority, and culture required to do the job entrusted to them by the President and Congress," said Amit Yoran, CEO of NetWitness Corp. and former director of the National Cyber Security Division at DHS. "DHS's cyber efforts are disorganized and disjointed, and practical operations continued to be buried deeper within the organization.

Bubonic Plague – Black Death

Estimated 30–60% of the European population was killed

Plague Timeline

Quarantine

224 BC

Hygiene

+1500 years

Vaccine

1796

2000 years to solve the problem?

200 years to reach population pre-plague

Unravel the Enigma of Insecurity

Elimination vs. Erradication vs. Control

Elimination

- The reduction of prevalence of a disease in a defined area to zero or the reduction of global prevalence to a negligible amount, e.g. Poliomyelitis and measles

1

Erradication

- The permanent reduction of the worldwide prevalence of a disease to zero, e.g. Smallpox

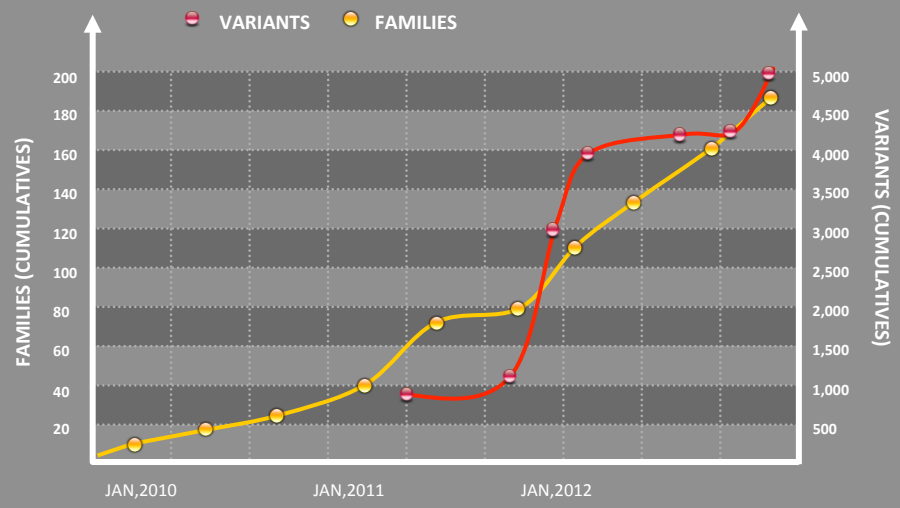
2

Control

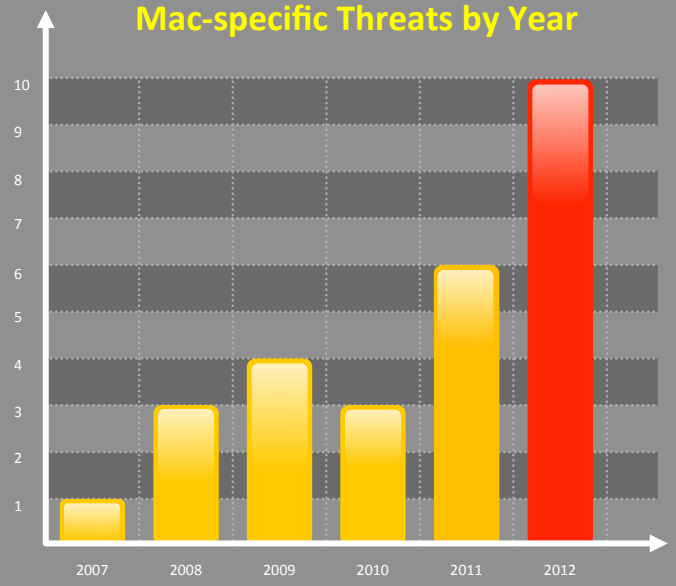
- The reduction in the incidence, prevalence, morbidity or mortality of an infectious disease to a locally acceptable level

3

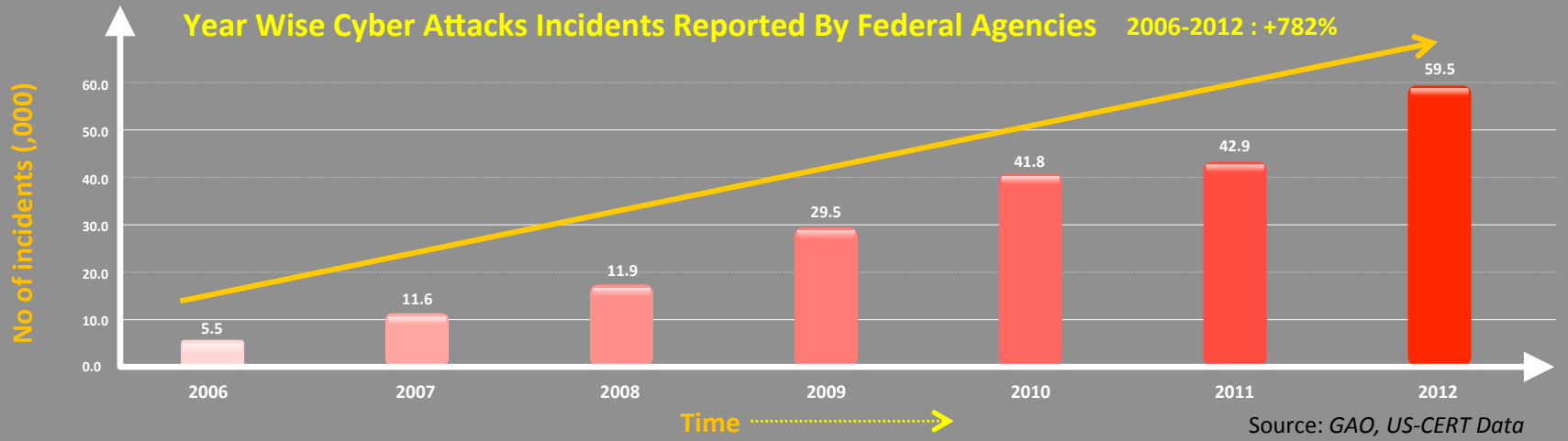
Cumulative Mobile Android Malware, 2010 to 2012



Mac-specific Threats by Year



Year Wise Cyber Attacks Incidents Reported By Federal Agencies 2006-2012 : +782%



Source: *GAO, US-CERT Data*

Unravel the Enigma of Insecurity

Timeline of Targeted attacks

Ghostnet
- March 2009
- Large-scale Cyber spying operation

Hydraq
- January 2010
- Operation "Aurora"

RSA Attacks

Stuxnet
- June 2010

Sykipot/Taidoor Attacks
- Targeting Defense Industry and Governments

Nitro Attacks
- July-October 2011
- Against Chemical Industry

Flamer and Gauss
- May 2012-Aug 2012
- Highly Sophisticated Threat
- Targets Middle East

Elderwood Project
- September 2012
- Main Target: Defense
- Same group identified using Hydraq(Aurora) in 2009

Puntos clave

- **Fiebre bubonica: elimino entre 30-60% poblacion**
- **Epidemia: 2,000 anos para solucion**
- **200 anos para recuperar la poblacion perdida**
- **Solucion: Eliminar, Erradicar, Controlar**
- **Tiempos entre problema y solucion**
- **Que tienen que ver las plagas con nosotros?**
- **Nuevas formas de plaga: Tecnologia, Internet**

The Massive Attacks

BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus

Plucky mail scrubbers battle internet carpet bombers

By John Leyden, 27th March 2013 *http://www.theregister.co.uk*

Anti-spam organisation Spamhaus has recovered from possibly the largest DDoS attack in history.

A massive 300Gbps was thrown against Spamhaus' website but the anti-spam organisation was able to recover from the attack and get its core services back up and running. CloudFlare, the content delivery firm hired by Spamhaus last week to guard against an earlier run of DDoS attacks, was also hit, forcing it into taking the highly unusual step of dropping London as a hub in its network - as a Twitter update by CloudFlare on Monday explained.

Our peering in London has been dropped due to a large attack. Modifying routes to avoid degradation. Affecting location: London, GB

Spamhaus supplies lists of IP addresses for servers and computers on the net linked to the distribution of spam. The blacklists supplied by the not-for-profit organisation are used by ISPs, large corporations and spam filtering vendors to block the worst sources of junk mail before other spam filtering measures are brought into play.

Spammers, of course, hate this practice so it's no big surprise that Spamhaus gets threatened, sued, and DDoSed regularly. Those affected by what they regard as incorrect listings also object about Spamhaus' alleged vigilante tactics.

RELATED STORIES

- Spamhaus-style DDoS attacks: All the hackers are doing it
- Rotten spam causing more infections than ever – study
- Call centers under attack in targeted cyber-blackmail scheme
- **Analysis** BIGGEST DDoS in history FAILS to slash interweb arteries
- **Analysis** Spamhaus and ISP spar over 'email DoS' blacklisting

Twitter: Hackers target 250,000 users

COMMENTS (251) *http://www.bbc.co.uk*

The BBC's technology correspondent Rory Cellan-Jones is one of those affected

A quarter of a million Twitter users have had their accounts compromised in the latest of a string of high-profile internet security breaches.

Twitter's information security director Bob Lord said about 250,000 users' passwords had been stolen, as well as usernames, emails and other data.

Related Stories

- Google boss on China 'IT menace'
- 'China hackers' attack NY Times
- China condemns NY Times 'smear'

Unravel the Enigma of Insecurity

The Massive Attacks

Apple suffers largest hacking attack in its history

By Jim Finkle and Joseph Menn
Reuters
Posted: 02/19/2013 11:40:58 AM PST
Updated: 02/19/2013 05:29:57 PM PST

BOSTON/SAN FRANCISCO -- Apple (AAPL) was recently attacked by hackers who infected Macintosh computers of some employees, the company said Tuesday in an unprecedented disclosure describing the widest known cyber attacks targeting Apple computers used by corporations.

Unknown hackers infected the computers of some Apple workers when they visited a website for software developers that had been infected with malicious software. The malware had been designed to attack Mac computers.

The same software, which infected Macs by exploiting a flaw in a version of Oracle's (ORCL) Java software used as a plug-in on Web browsers, was used to launch attacks against Facebook, which the social network disclosed on Friday.

The malware was also employed in attacks against Mac computers used by "other companies," Cupertino-based Apple said, without elaborating on the scale of the assault.

More Apple coverage

- Apple, Google, Faceb deny giving NSA, FBI to servers
- Cupertino: Apple's ne headquarters will gen 'unacceptable level' o 280, report says
- Officials to seek cure smartphone thefts in Apple, Google
- Apple said to begin iP this month
- Apple to sell audio ad music service, source

http://www.mercurynews.com

Infecting MAC Computers

Chameleon botnet steals $6M per month in click fraud scam

More than 120,000 Windows-based computers running Internet Explorer 9 are infected in the U.S., researchers say.

by Steven Musil | March 19, 2013 8:55 PM PDT
Follow @stevenmusil

http://news.cnet.com

140 0 12 +1 17 More + Comments 0

Security researchers say they have identified a botnet that steals more than $6 million per month by generating fake customer clicks on online display ads.

Dubbed Chameleon, the botnet has infected more than 120,000 Windows-based computers in the U.S., mimicking human behavior on select Web sites to generate billions of ad impressions and fraudulent income for its creators, according to security firm Spider.io.

Click fraud costs Web advertisers in lost revenue by making them pay for illegitimate clicks. Spider.io reported that advertisers paid an average of 69 cents per one thousand impressions generated by the botnet. Researchers estimate Chameleon was responsible for two-thirds of the 14 billion ad impressions served by the 202 affected Web sites, nearly all of which are located in the U.S.

Unravel the Enigma of Insecurity

Chinese hackers steal U.S. weapons systems designs, report says

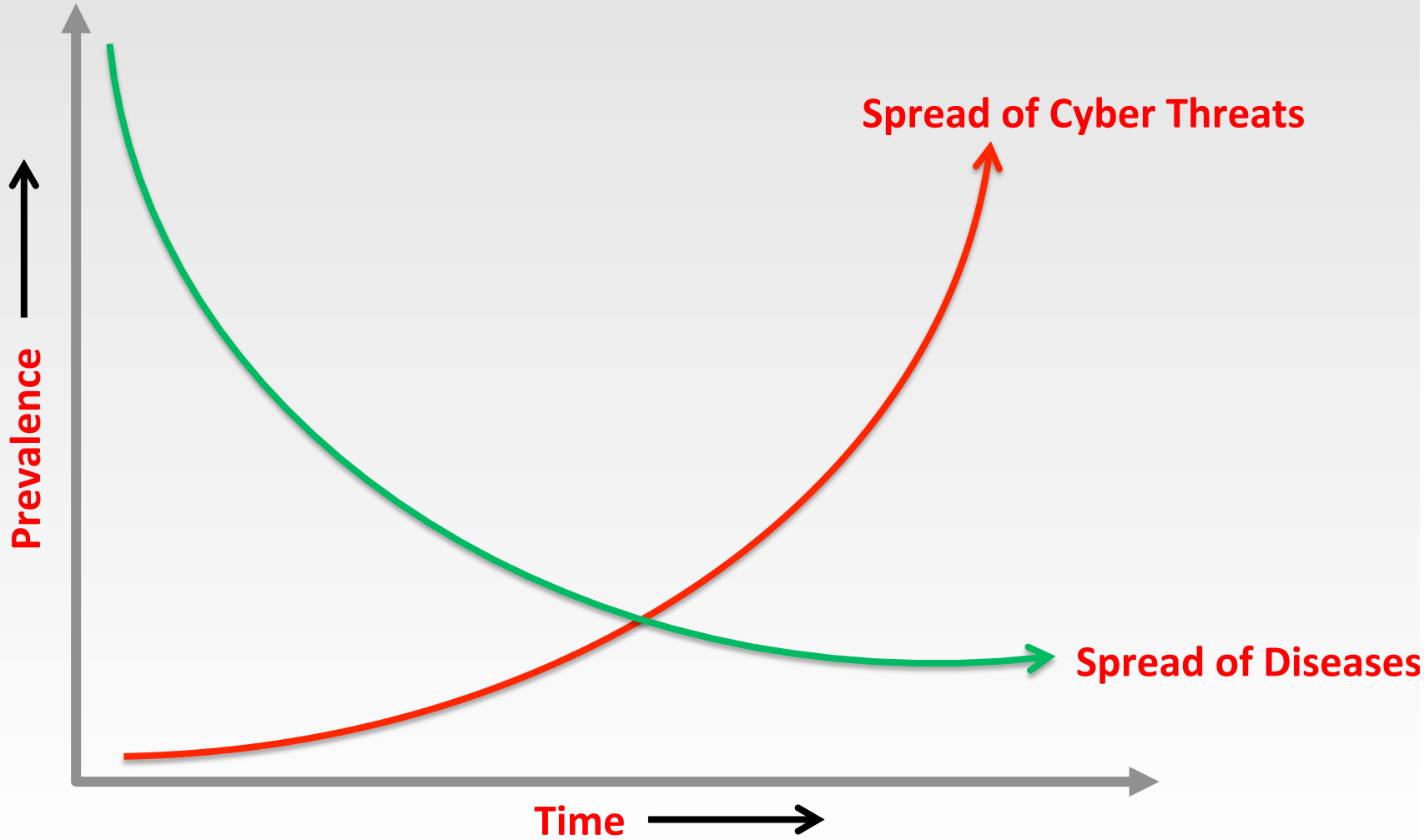
This image provided by the US Navy shows a modified Standard Missile 2 interceptor is launched in 2008 from the guided-missile cruiser USS Lake Erie during a test. A new report says Chinese hackers have stolen designs for several U.S. weapons systems.

By Terril Yue Jones, Bill Trott and Rob Taylor, Reuters

Chinese hackers have **gained access to designs of more than two dozen major U.S. weapons systems**, a U.S. report said on Monday, as Australian media said Chinese hackers had stolen the blueprints for Australia's new spy headquarters.

Citing a report prepared for the Defense Department by the Defense Science Board, the Washington Post said the compromised U.S. designs included those for combat aircraft and ships, as well as missile defenses vital for Europe, Asia and the Gulf.

An Analogy: WE ARE LOSING THE FIGHT !



Cyber Plague

You are in IT !!!!!!!

Large Giants being taken out with hacks invented a long time ago

LinkedIn facebook

CHASE

Microsoft

The New York Times

SONY
make.believe

Cyberplague Timeline

Quarantine

Firewall

IDS

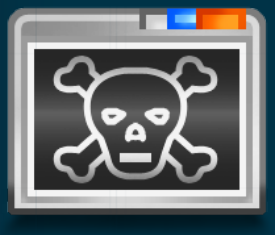
IPS

Cyber Hygiene

Education

Policy

Vaccine



Unravel the Enigma of Insecurity

Puntos clave

- **Enfermedades Humanas y enfermedades virtuales**
- **Humanas – Desprotegidos**
- **Virtuales – Todos (Grande, reconocido, mayor)**

- **Estamos perdiendo!**
- **Antiguas soluciones: Cuarentena, Higiene**
- **Aun no hay vacuna**

Wrong Code vs. Correct Attack

Vulnerable Code (Non-Parameterized stored procedure)

```
1: Try
2: Dim command As SqlCommand = new
   SqlCommand("sp_getAccountBalance(CustomerName.Text)", connection);
3: Dim reader As SqlDataReader = command.ExecuteReader();
4: Catch se As SqlException
5: ' error handling
6: End Try
```

Vulnerable to **SQL injection attack**

This parameterized stored procedure approach helps in **preventing SQL injection attacks**

Secure Code (Parameterized stored procedure)

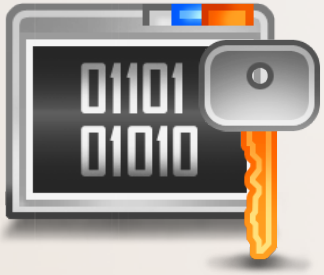
```
1: Try Dim command As SqlCommand = new SqlCommand("sp_getAccountBalance", connection);
2: command.CommandType = CommandType.StoredProcedure;
3: command.Parameters.Add(new SqlParameter("@CustomerName", CustomerName.Text));
4: Dim reader As SqlDataReader = command.ExecuteReader();
5: Catch se As SqlException
6: ' error handling
7: End Try
```

Type's of Vaccine

ACTIVE IMMUNIZATION
Measles, Mumps, Yellow Fever, Rotavirus

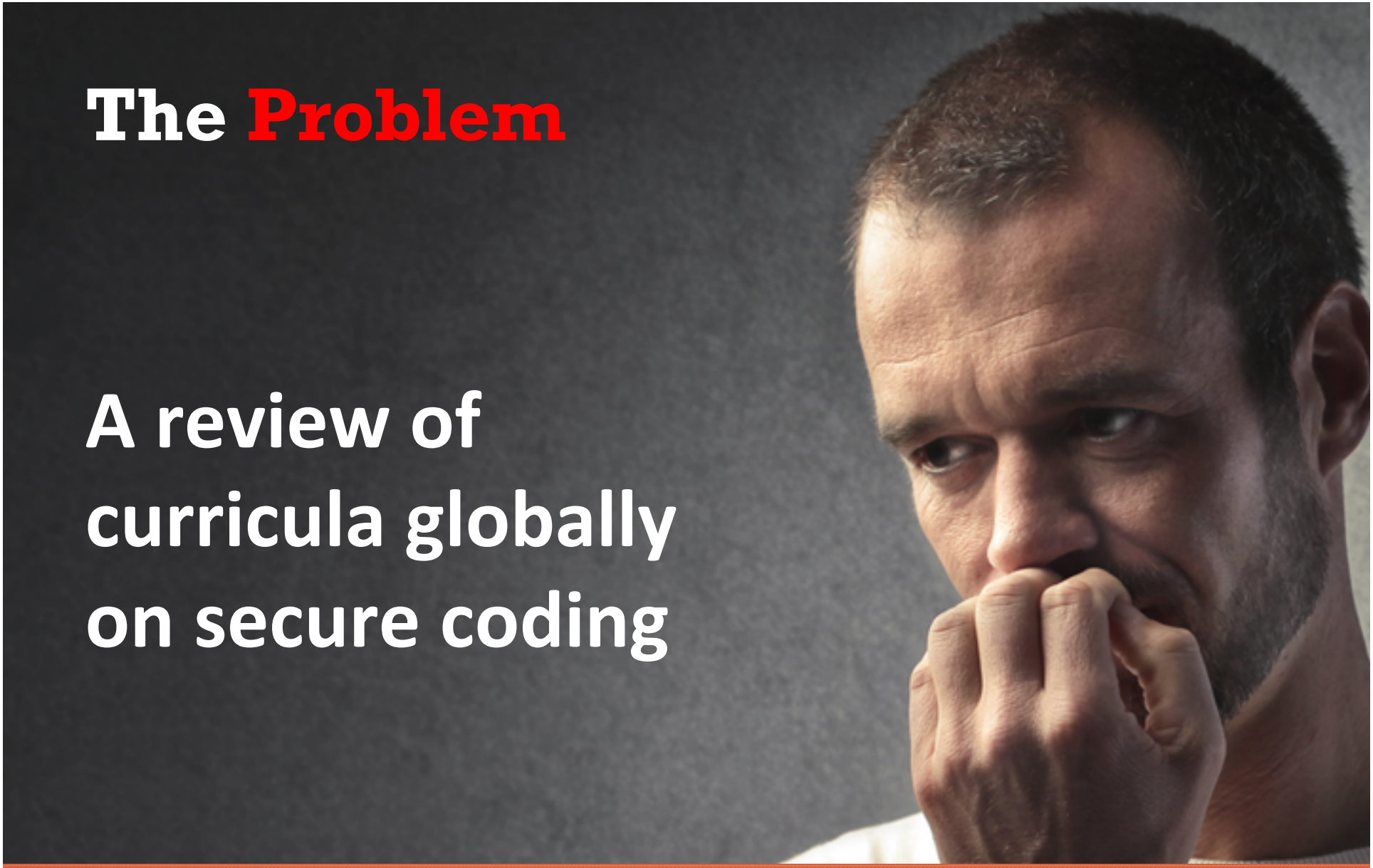
Ethical Hacker (Antigen and Antibody)

PASSIVE IMMUNIZATION
Tetanus



Secure Code (Antibody)
Immunological Memory

The Problem



A review of curricula globally on secure coding

Unravel the Enigma of Insecurity

Secure Coding Education: Are We Making Progress?

> "While current computer science (CS) programs are adept at teaching programming skills including exposing students to languages commonly used in industry, the focus is often on "making programs work". Students are typically given an assignment with a set of functional goals such as to create a program that reads records from a file, and then performs some calculation based on the values retrieved. In such cases little consideration is given to secure programming issues, and as such students do not learn how to write programs that would be resilient to accidentally or maliciously malformed input in real world conditions."
>
> - *Proceedings of the 16th Colloquium for Information Systems Security Education. 2012*

World's Best Universities

No Comprehensive Secure Coding Program

The Point

The Vaccine

Secure Coding

Manufacturing the Panacea

Unravel the Enigma of Insecurity


1
All India Secure Coding Competition 2013
2
Across Universities All Over India
3
Preliminary, Semi Finals, and Final
4
We want HOD across Universities to be part of it
EC-Council Code | Uncode
Researching India
Unravel the Enigma of Insecurity

Code Uncode Partnerships

NASSCOM®

IT AP
The IT and ITES Industry Association of AP
(Formerly HYSEA)

HCL

Aspro Technologies

modi naturals
Oleev
Go beyond

Seeroo
IT SOLUTIONS Pvt. Ltd.
Powerful Thoughts • Simple Solutions

SRISHTI INNOVATIVE
Quality Beyond Contract

NANO SOFTWARES
Quality Guaranteed

COMPUTER SOCIETY OF INDIA
ESTD. 1965

KRYONNS
Technologies

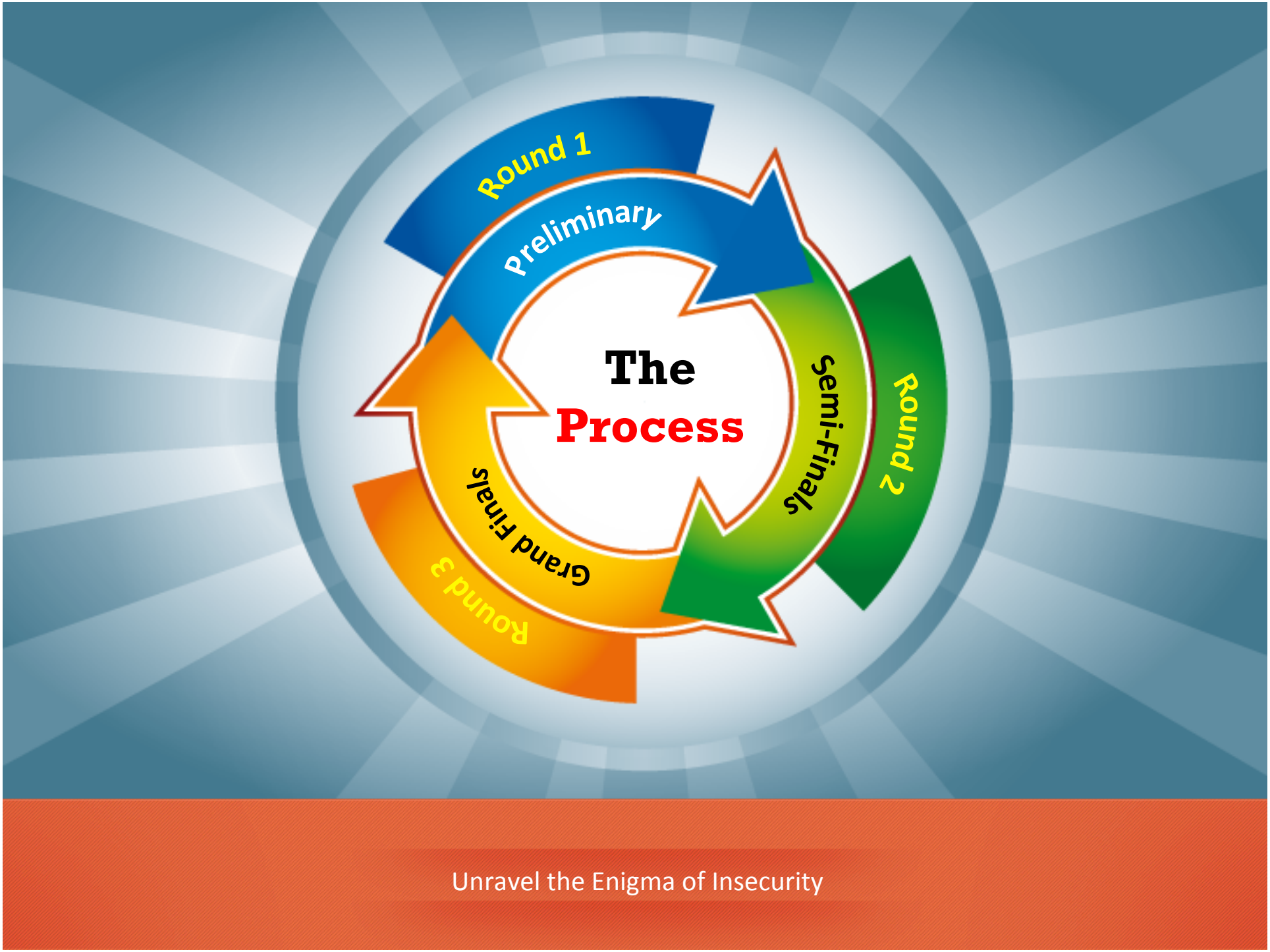
SYNERZIP
Agile Software Product Development Partner

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education Transforming India

THAPAR UNIVERSITY

AMITY UNIVERSITY

neptune
Neptune Software Group



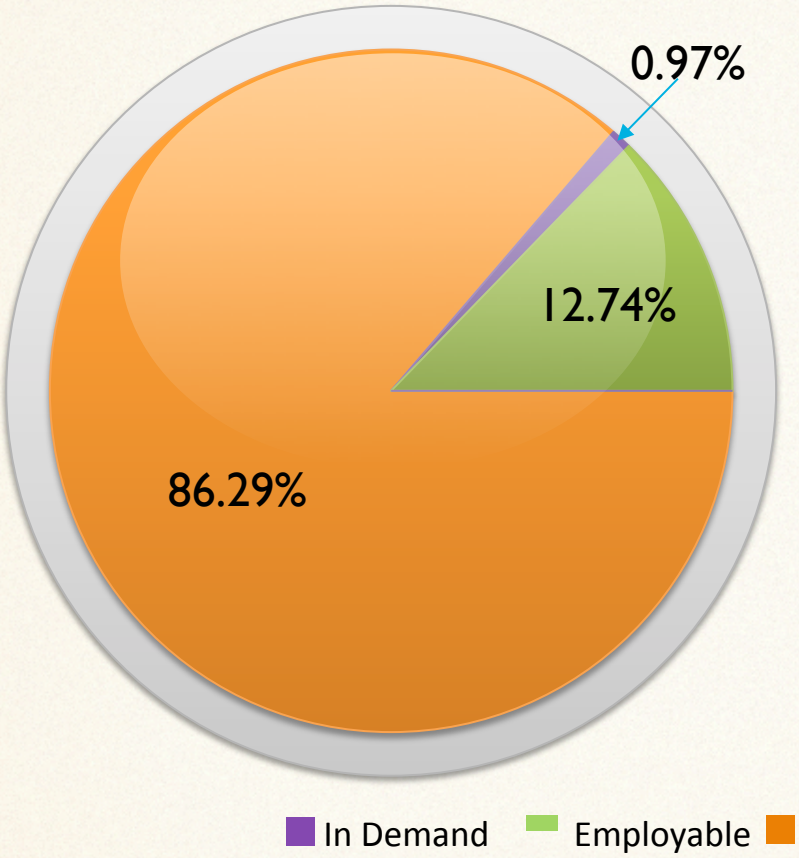
Unravel the Enigma of Insecurity

The Result!!!

Unravel the Enigma of Insecurity

Lessons Learnt

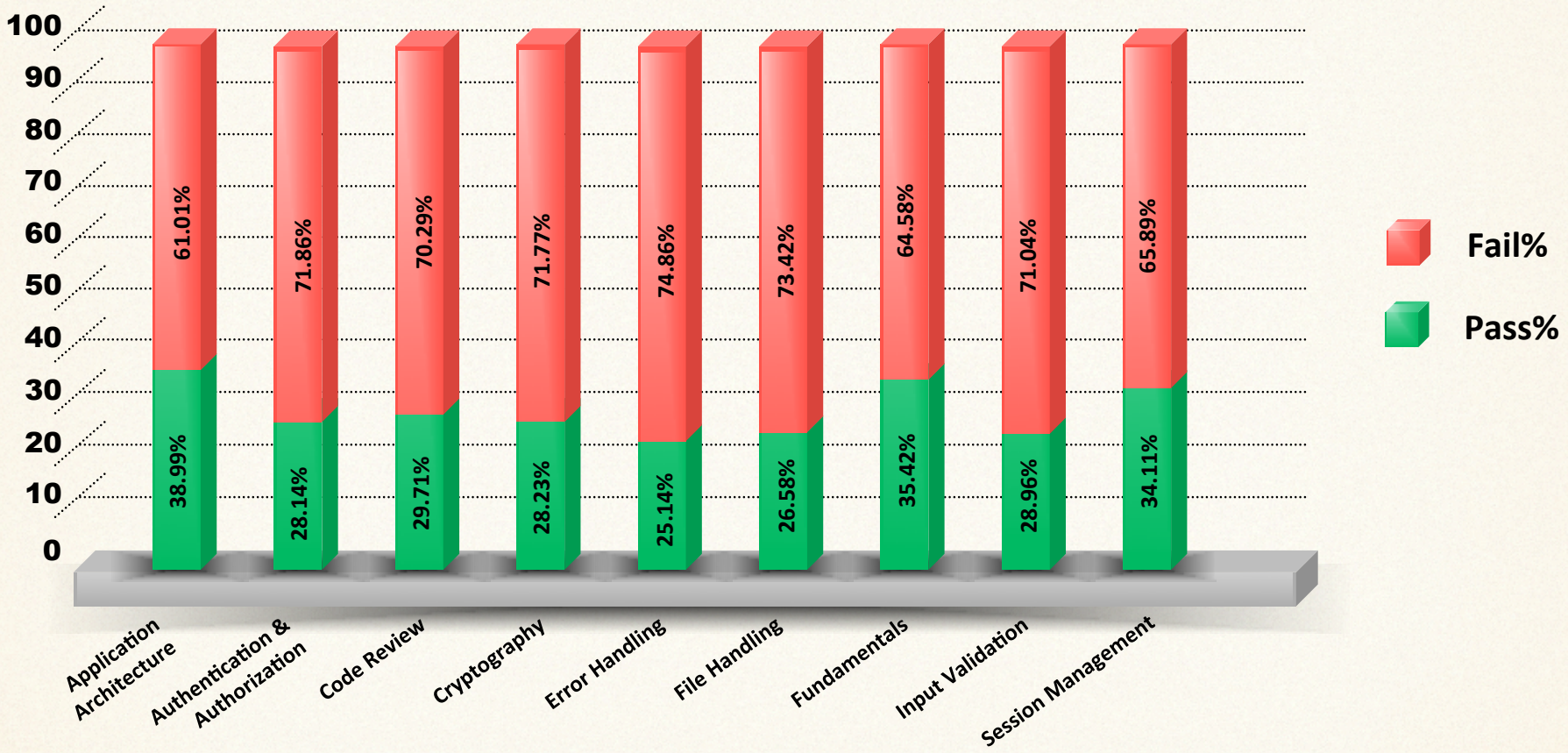
All India – Skill Level Analysis



India's talent pipeline in **Secure Coding** skills emerges at its weakest with just under a percentage of student population in engineering equipped with **basic skills** in **Secure Coding**

Lessons Learnt – Identifying the Gaps

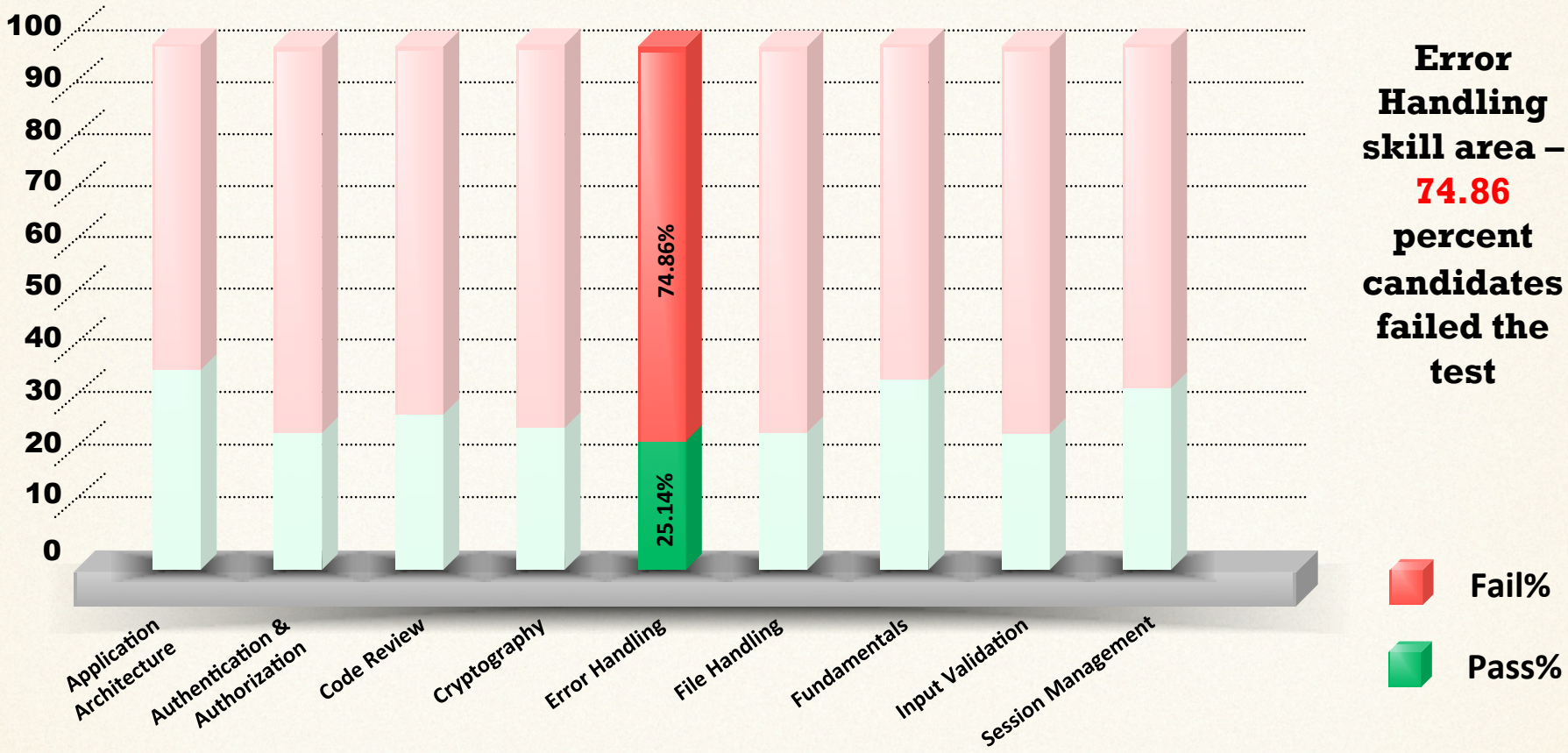
Performance of the candidates in individual skill categories



Identifying the Gaps – What Does It Mean?

Improper handling of errors and exception makes you vulnerable to:

- Disclosure of sensitive information
- Denial-of-service attacks



Error Handling skill area – 74.86 percent candidates failed the test

Cybercrooks Use DDoS Attacks to Mask theft of Banks' Millions

Distributed denial of service attacks have been used to divert security personnel attention while **millions of dollars were stolen from banks**, according to a security researcher.

At least three US banks in recent months have been plundered by fraudulent wire transfers while hackers deployed "low powered" **DDoS attacks** to mask their theft, Avivah Litan, an analyst at research firm Gartner, told SCMagazine.com. She declined to name the institutions affected but said the attacks appeared unrelated to the wave of DDoS attacks last winter and spring that took down Web sites belonging to JP Morgan , Wells Fargo, Bank of America, Chase, Citigroup, HSBC, and others.

http://news.cnet.com

DoS/DDoS attack due to Improper Exception Error handling and Poor Input Validation

GCSB website attacked by hackers today

By Brendan Manning

7:04 PM Friday Aug 23, 2013 ☆ Save 29 44

The Government Communications Security Bureau website was attacked by hackers earlier today.

A spokesman for the organisation said although the attack did not shut down the website, it slowed the website's gateway for about 30 minutes.

"... There is an indication there could have been some temporary degradation of service."

Prime Minister John Key. Photo / Mark Mitchell

It is believed the website suffered a DDoS or distributed denial-of-service attack, where a website suffers a saturation of external communications requests to the point that it cannot respond to legitimate traffic in an attempt to cause the server to overload.

The attack did not affect GCSB operations in any way the spokesman said.

A Twitter page with the handle 'OpF*ckGCSB' tweeted "#TangoDown" and a screen shot showing the website down.

The Twitter user claimed links to the international 'hacktivist' group Anonymous.

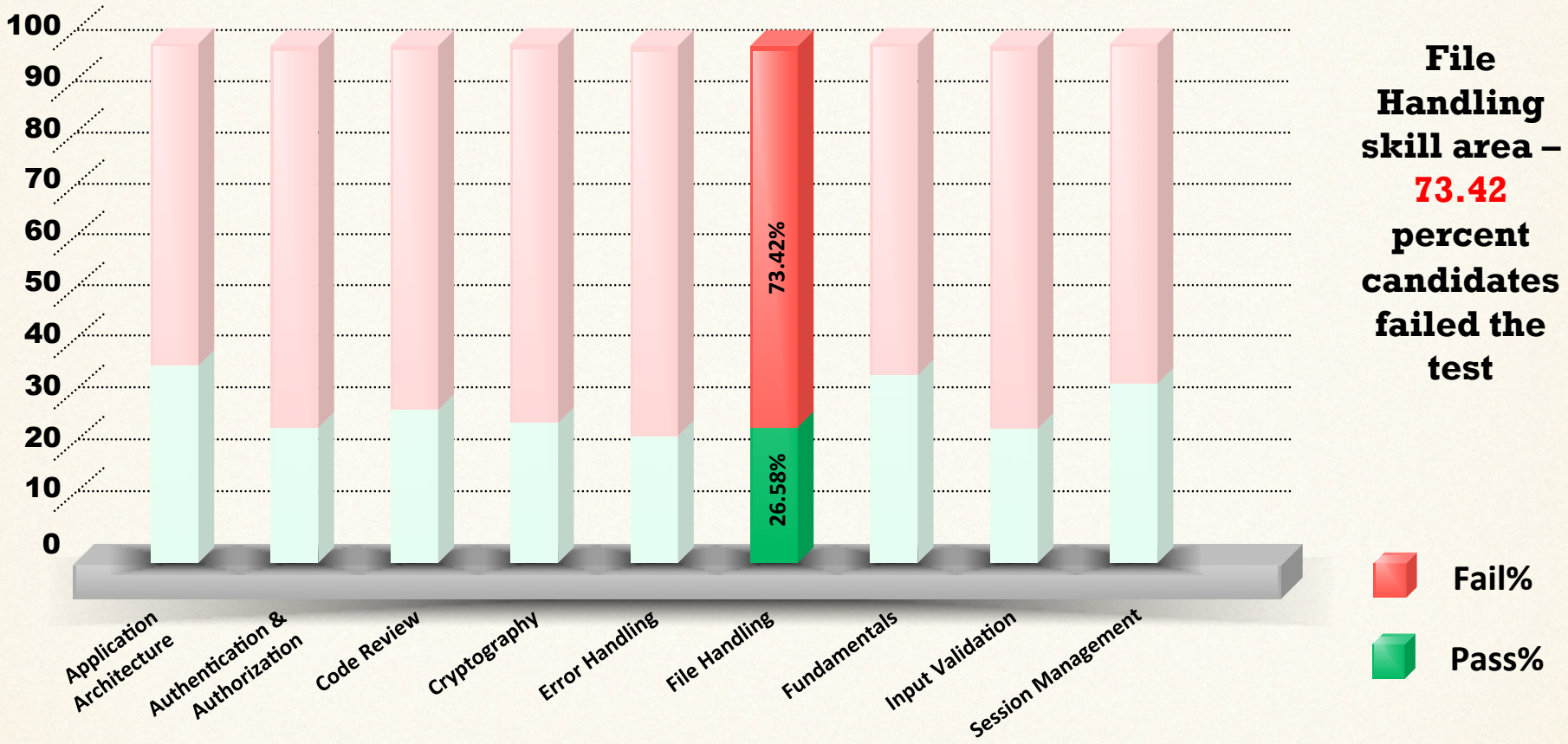
- APNZ

By Brendan Manning Brendan

Identifying the Gaps – What Does It Mean?

Insecure file handling makes you vulnerable to:

- Malicious file Inclusion; malware distribution
- DoS/DDoS attacks



File Handling skill area – 73.42 percent candidates failed the test

Sensitive Information Disclosure due to Insecure Data Storage

Officials: Public Disclosure Commission hacked

Washington agency provides public access to campaign data

By Rachel LaCorte, Associated Press

Tuesday, September 17, 2013

Recommend 0 Send Tweet 0 +1 0 Pin it Digg submit

OLYMPIA — The state Public Disclosure Commission's network was breached earlier this month, though officials on Tuesday said no information was compromised.

Michael Smith, chief technology officer for the state agency, said that the agency was notified by the state's Consolidated Technology Services last week that a virus had hit the network on Aug. 17, but that the actual network incursion occurred on Sept. 8.

Smith says that the PDC was told by CTS that the incursion was initially believed to be domestic, but may have been done by a foreign government. Smith said no sensitive information was obtained or changed on the system, which contains financial records that are public records. The commission provides public access to information about financing of political campaigns and lobbying activities.

"We believe it was mostly for a reconnaissance mission to identify machines on our network," Smith said.

However, David Postman, a spokesman for Gov. Jay Inslee, said that there was no evidence of foreign involvement.

"Often, it is a possibility that an attack can come from overseas, but in this case we are certain there is no good evidence that this was any foreign government," Postman said in an emailed response. "There were foreign IP addresses, which is quite common in hacking attacks. This is considered a lower level attack."

Smith said that CTS was notified of the breach by the FBI, which saw some of the agency's usernames and passwords on a reputed hacker's website. Since the agency learned of the hacking, Smith said that passwords have been changed, and CTS has been scanning their sites looking for potential points of vulnerability.

The FBI is currently analyzing the breach, Smith said, but, Postman said that the FBI was not involved.

In an email, FBI spokeswoman Ayn Dietrich said she could neither confirm nor deny any investigation, but wrote "the public should be assured that the FBI takes seriously cyber intrusions that could compromise national security."

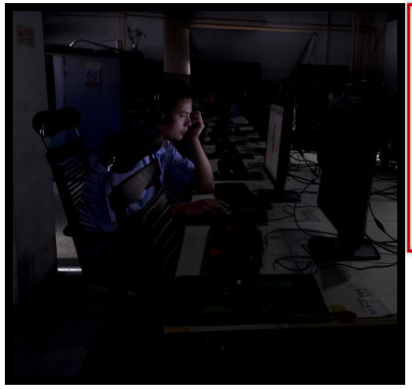
This is the second known data breach in Washington state this year.

China hit by massive Web attack this weekend

Over the weekend, .cn – the Chinese equivalent of .com – went dark, according to reports by the China Internet Network Information Center.

By Katherine Jacobsen, *Contributor* / August 26, 2013

Every website that uses the .cn suffix was inaccessible for several hours over the weekend, the result of "the largest ever" hack on Chinese sites, according to the China Internet Network Information Center (CNNIC).

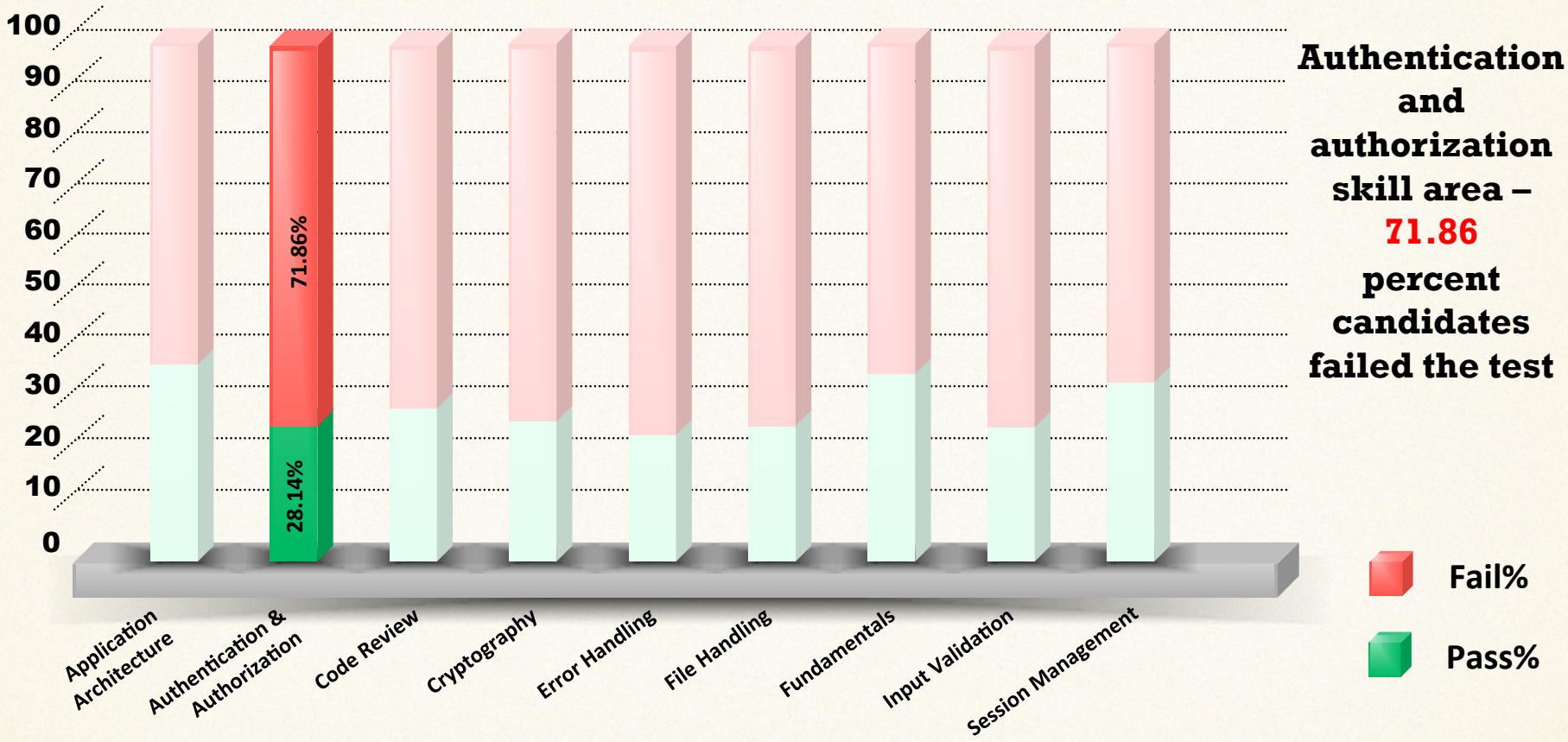


Before malicious coders can launch a DDoS attack, they must infect the computers of unsuspecting users, often by tricking people into installing malware on their computers. The malware can then be coordinated to attack a website or network, and an off-site controller can launch the attack at his or her choosing, flooding the servers with a stream of hits. This effectively causes the site to collapse, or at least become useless for a few hours. Though the .cn domain was down, many service providers store parts of the online registry, so some .cn websites could have still been accessible to users, according to CloudFlare, an online content delivery network. Furthermore, the relative ease of spreading viruses means that the attack could have been perpetrated by an individual.

Identifying the Gaps – What Does It Mean?

Improper authentication and authorization makes you vulnerable to:

- Credential theft
- Eavesdropping
- Brute-force and dictionary attacks
- M-I-T-M attack
- Data tampering
- Account hijacking
- Information leakage
- Disclosure of confidential data
- Privilege escalation
- Luring attacks



Authentication and authorization skill area – 71.86 percent candidates failed the test

Man-in-the-Middle(MITM) attack due to poor Implementation of Authentication and Authorization mechanism

NSA disguised itself as Google to spy, say reports

If a recently leaked document is any indication, the US National Security Agency -- or its UK counterpart -- appears to have put on a Google suit to gather intelligence.

by Edward Moyer | September 12, 2013 2:19 PM PDT

Follow

Here's one of the latest tidbits on the NSA surveillance scandal (which seems to be generating nearly as many blog items as there are phone numbers in the spy agency's data banks).

Earlier this week, Techdirt picked up on a passing mention in a Brazilian news story and a Slate article to point out that the US National Security Agency had apparently impersonated Google on at least one occasion to gather data on people. (Mother Jones subsequently pointed out Techdirt's point-out.)

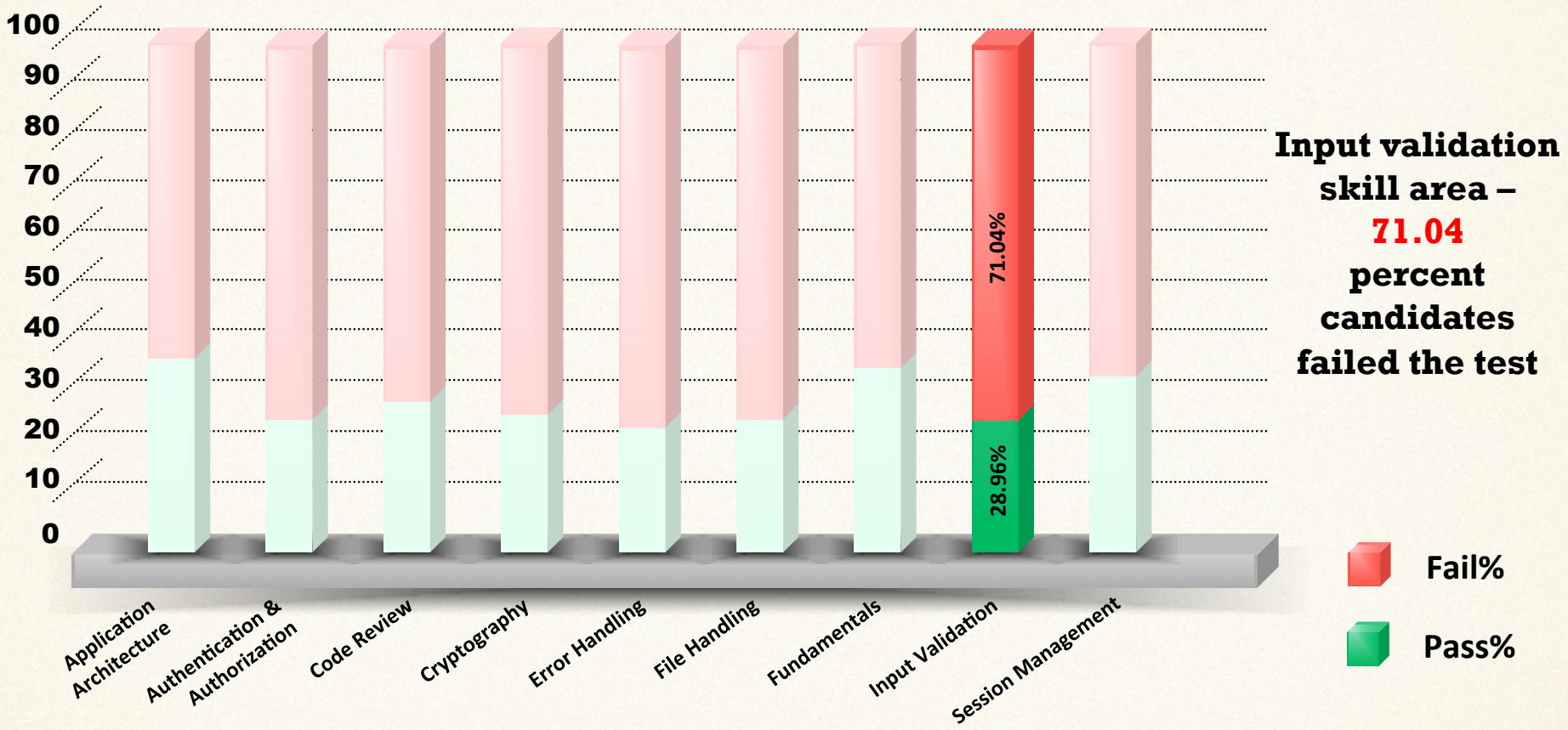
Brazilian site Fantastico obtained and published a document leaked by Edward Snowden, which diagrams how a "man in the middle attack" involving Google was apparently carried out.

A technique commonly used by hackers, a MITM attack involves using a fake security certificate to pose as a legitimate Web service, bypass browser security settings, and then intercept data that an unsuspecting person is sending to that service. Hackers could, for example, pose as a banking Web site and steal passwords.

Identifying the Gaps – What Does It Mean?

Improper input validation makes you vulnerable to:

- Buffer overflow
- SQL injection
- Cross-site request forgery
- Cookie manipulation
- Query string manipulation
- HTTP header manipulation
- Unvalidated Redirect
- Cross-site scripting
- Canonicalization attacks
- Form field manipulation



Input validation skill area – 71.04 percent candidates failed the test

Unvalidated Redirect/Website Defacement attack due to Poor Input Validation

Syrian Electronic Army attacks Marines website saying 'Obama is a traitor'

Message to the United States Marine corps:

Dear US Marines,

This is a message written by your brothers in the Syrian Army, who have been fighting Al Qaeda for the last 3 years.

We understand your patriotism and love for your country so please understand our love for ours.

Obama is a traitor who wants to put your lives in danger to rescue Al Qaeda insurgents.

Marines, please take a look at what your comrades think about Obama's alliance with Al Qaeda against Syria.

I Will NOT Fight for Al Qaeda In Syria

Your officer in charge probably has no qualms about sending you to die against soldiers just like you,

fighting a vile common enemy. The Syrian army should be your ally not your enemy.

Refuse your orders and concentrate on the real reason every soldier joins their military,

Screenshot of Marines.com

September 2, 2013 1:52 PM

Meghan Kelly

2 Comments

Like 60 +1 2 Tweet 60 Share VB More

The Syrian Electronic Army hit the Marines' recruiting website today, redirecting visitors to a separate website with images depicting "soldiers" who are against a military strike on Syria.

The SEA is a group of pro-regime hackers who most often target publications for their coverage of the conflict in Syria. The group often defaces websites or redirects them to its own website as an attempt to get their own messaging and propaganda across. Recently, the group reportedly hacked into Melbourne IT, a domain name registrar, and was able to take down the New York Times website.

Website Defacement attack due to Poor Input Validation

Brazilian hackers attack NASA website instead of NSA in retaliation for US 'snoop-op'

The hackers left a message on the site that read, 'Stop spying on us'

Learn Ethical Hacking
Certified Ethical Hacker Courses by Koenig Solution Limited www.Koenig-India.com
Ads by Google

Like 17 Tweet 4 +1 1 Share 1 Share 1 Add to My Page

Read more on: Nasa | Brazil | Nsa | Hacking | Us | Snowden

RELATED NEWS

- Brazilian president's state visit to US postponed
- BASIC nations agree with India's stand on HFCs
- Brazil hackers mistake NASA for NSA in spying payback
- Kashmiri origin girl has only one dream--to be a commercial
- Platini may run for FIFA presidency in 2015

Learn Ethical Hacking
Ethical Hacking Training Program
Hacking Hackers
www.innobuzz.in/Hacking

Microsoft Dynamics
Business Solutions as Unique as

Brazilian hackers mistook the US space agency NASA for the country's spy agency NSA, and hacked it in retaliation of the alleged US 'snoop-op' on Brazil.

Brazilian news portol Uol said that some activists decided to protest the US practice but picked the wrong target and hacked NASA's website with a message that read, 'Stop spying on us' and also called on the US to not attack Syria.

Nasa spokesperson Allard Beutel confirmed the attack but said that none of the agency's primary websites, missions or classified systems were compromised, News24 reports.

The spokesperson further added that the agency was diligently taking action to investigate and reconstitute the websites impacted during web defacement incident.

According to the report, the classified documents leaked by NSA whistleblower Edward Snowden indicated that the US spy agency allegedly snooped on Brazilian President Dilma Rousseff's e-mail communications and on the state-run energy giant Petrobras.

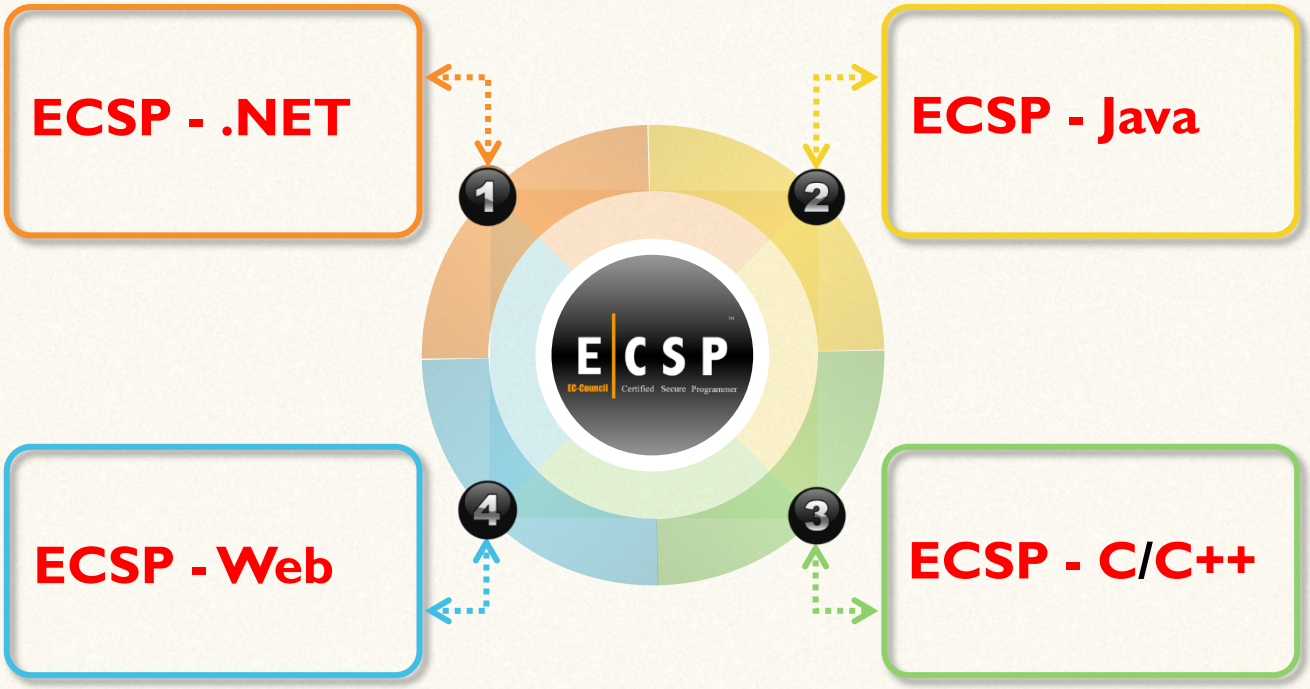
Brazil, slamming the alleged surveillance programmes as 'unacceptable', demanded explanations from Washington.

Why the Gap is Dangerous – A Summary

Category	Attacks		
Poor Input and Data Validation	Buffer overflow Cross-site scripting SQL injection	Cross-site request forgery Canonicalization attacks Query string manipulation	Form field manipulation Cookie manipulation HTTP header manipulation
Poor Authentication and Authorization Mechanism	Credential theft Eavesdropping Privilege escalation	Brute-force and dictionary attacks Man-in-the-Middle attack Disclosure of confidential data	Account hijacking Information leakage Data tampering
Insecure Data Storage	Accessing sensitive data in storage and memory	Data tampering	Network eavesdropping
Poor Session Management	Session hijacking	Man-in-middle attacks	Session replay
Insecure Exception and Error Handling	Disclosure of sensitive information	Denial-of-service attacks	
Poor Configuration Management	Illegal access to administration Interfaces	Illegal access to configuration stores	Theft of clear text configuration secrets
Weak Cryptography	Loss of decryption keys	WEP Encryption cracking	
Improper Auditing and Logging	Denial of performing an operation by user	Exploitation of an application by an attacker without trace	Covering tracks
Improper File Handling	Malicious file Inclusion	DoS/DDoS attacks	

What EC-Council is Doing to Fill the Gap

ECSP – The Vaccine



EC-Council's **comprehensive secure programming training** programs

Solution:

Start Manufacturing the Panacea now!

INSERT NICE FORMAT

University World News
The global window on higher education

Receive our free newspaper

15 February 2009

EUROPE: Universities must address information security

Writer: Paul Cochrane
Date: 05 October 2008

Information technology security training at European universities was an aspect of the university curriculum that institutions needed to address, participants were told at a conference organised by the European Network and Information Security Agency, Enisa, last month in Crete.

"Universities have started to work on courses and are defining security but we can do more in terms of programmes," said Professor Evangelos Markatos of the Institute of Computer Science of the Foundation for Research and Technology. "There needs to be a new generation of security engineers, and security has to be thought about from the beginning."

Courses that are offered, such as those at Britain's Cambridge University and Royal Holloway College at the University of London, also needed to train students for security issues in the work place, said Paul Dorey, Director of Digital Security with oil company BP.

"It helps engineers when training to think about security. Courses are being given but there is not enough awareness of standard IT security. Many large companies often have to retrain programmers, such as at banks in secure programming," Dorey said.

Markatos said universities were sensitive to hacking and cyber crime, and usually had systems in place to rapidly find such cases and stop them from spreading within the university's IT infrastructure.

While universities were updating techniques to respond to cyber attacks, institutions were also playing a vital role in raising awareness of IT security and protection through partnerships with European ministries of education and the private sector, said Isbaella Santa, Senior Expert at Enisa.

"Such an approach, of public-private partnerships, is better than say Microsoft doing it, as people would say, trying to sell software," she said. "Some universities in Germany are also offering courses on the psychological effects of stolen data, whether children are addicted to computing, and other social aspects of e-security."

Related Links
About University World
Other articles by Paul Cochrane
Other articles from European Union
More Business
Newsletter Archives

Most Popular Articles
SOUTH AFRICA: Student drop-out rates alarming
CHINA: Chinese students to dominate world market
SOUTH AFRICA: Universities set priorities for research
OECD: Worldwide 'obsession' with league tables
UK: Few surprises in new THES rankings
FRANCE: Smallest university created
UK: Two centuries of honours degrees to disappear
US: Keeping stem cell research alive
OECD 1: US share of foreign students drops
AUSTRALIA: Research quality scheme scrapped

डॉ0 आर. मनोज कुमार
शिक्षा अधिकारी

Dr. R. Manoj Kumar
Education Officer

ज्ञान-विज्ञान विमुक्तये

विश्वविद्यालय अनुदान आयोग
बहादुरशाह जफर मार्ग,
नई दिल्ली – 110 002
UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002

Phone : 011-23
E-Mail: rmku

BY SPEED POST

D. O. No.14-7/2009(CPP-II) 16th January, 2013

Dear Madam/Sir,

Subject: Introduction of Cyber Security/Information Security as a subject.

This is with reference to the recommendation of the Task Force on National Security System constituted on the direction of the Cabinet Committee on Security. The Task Force has made the following recommendation:-

UGC and AICTE would ensure that Cyber Security/Information Security is introduced as a subject in the universities/technical institutions at the under-graduate and post-graduate levels.

Therefore, I am directed to request you to take appropriate action on the above recommendation. This may also be brought to notice of the colleges, if any, affiliated to your university.

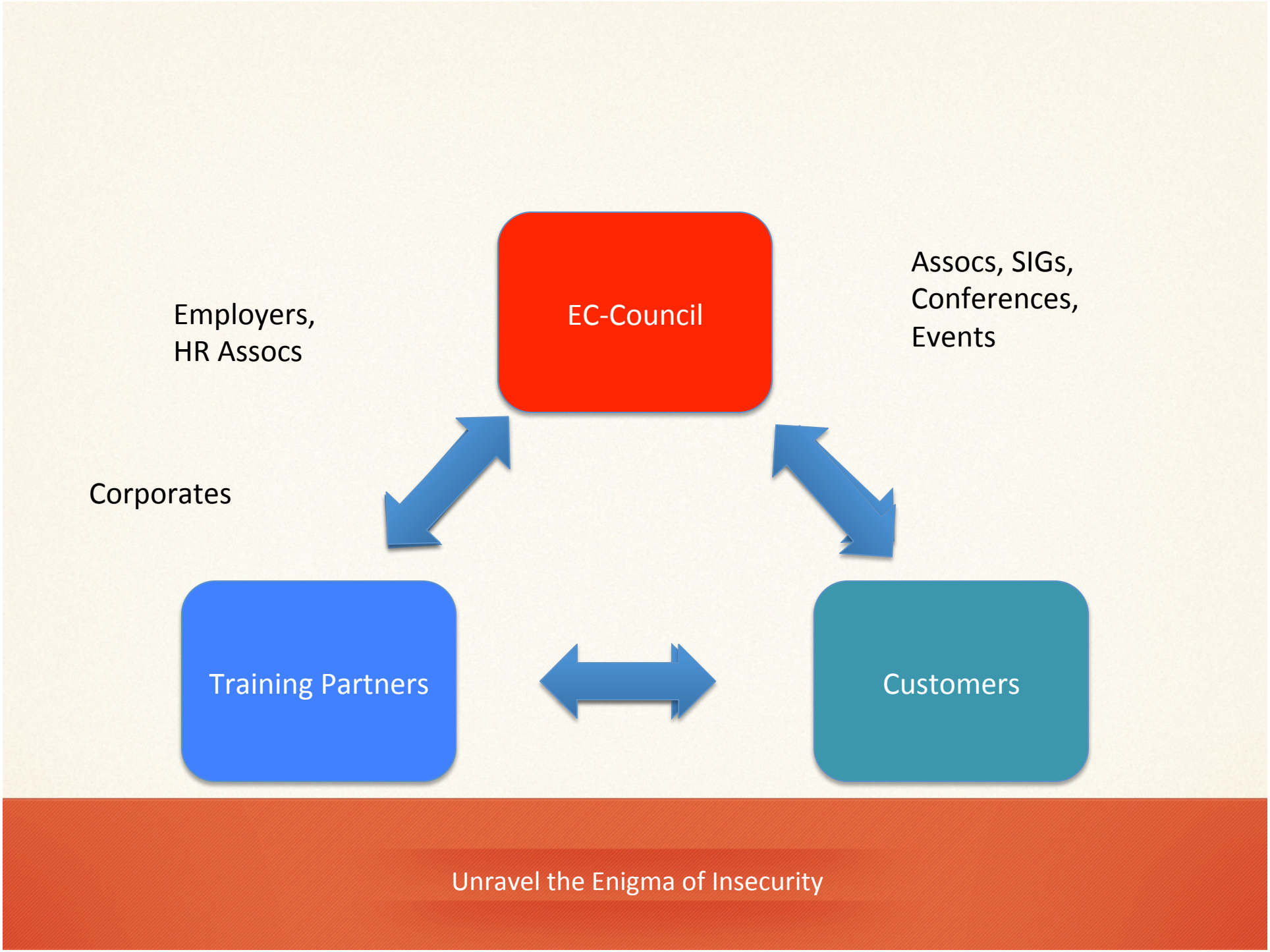
Yours faithfully,

(**R. Manoj Kumar**)
Education Officer

To
All Vice-Chancellor

Critical and immediate Remediation of lack of IS Knowledge from India's Education Authority.

Unravel the Enigma of Insecurity


Employers,
HR Assocs
EC-Council
Assocs, SIGs,
Conferences,
Events
Corporates
Training Partners
Customers
Unravel the Enigma of Insecurity