

# Information Security: What is done and what is to be done?

*Igor Mkrtumyan*  
*Internet Society - Armenia*  
*e-mail: [imkrtumyan@isoc.am](mailto:imkrtumyan@isoc.am)*

# What is done?

- Document on “What is done?” is distributed
- Briefly:
  - CERT AM and AM NREN CSIRT were created with the help of CEENet/NATO
  - Some equipment was received by AM NREN CSIRT from CEENet/NATO to be used to provide BSI project security
  - About 10 information security officers were trained
- CERT AM web site was created
- [infosec@cert.am](mailto:infosec@cert.am) mailing list was started providing useful information to subscribers
- Sysadmin leaflets on security are sent to the mailing list
- CISCO Security trainers were trained for ISOC AM Cisco Academy
- Cisco Security bundle was received from CEENet

# What is to be done?

## Problems:

- Antivirus software
- Antispyware
- Web sites' security
- Forming the Community
- CERT AM activity
- Introduction of ISO standards on security

# Attack Methods

Abuse of Functionality

Administration Error

Brute Force

Buffer Overflow

Content Spoofing

Credential/Session Prediction

Cross Site Request Forgery (CSRF)

Cross Site Scripting (XSS)

Denial of Service

Directory Indexing

Drive by Pharming

Failure to Restrict URL Access

Format String Attack,

HTTP Response Splitting

Improper Error Handling

Insecure Direct Object Reference

Insufficient Anti-automation,

Insufficient Authentication

Insufficient Authorization

Insufficient Process Validation

Insufficient Session Expiration  
Known Vulnerability  
LDAP Injection  
Misconfiguration  
OS Commanding  
Other  
Path Traversal  
Predictable Resource Location  
Redirection  
Session Fixation  
Session Hijacking  
SQL Injection  
SSI Injection  
Unintentional Information Disclosure  
Unknown  
Weak Password Recovery Validation  
XPath Injection

# New web hacking techniques

CUPS Detection

CSRFing the uTorrent plugin

Clickjacking / Videojacking

Bypassing URL AuthC and AuthZ with

HTTP Verb Tampering

I used to know what you watched, on YouTube

Safari Carpet Bomb

Flash clipboard Hijack

Flash Internet Explorer security model bug

Frame Injection Fun

Free MacWorld Platinum Pass? Yes in 2008!

Diminutive Worm, 161 byte Web Worm

SNMP XSS Attack

Res Timing File Enumeration Without

JavaScript in IE7.0

Stealing Basic Auth with Persistent XSS

Smuggling SMTP through open HTTP proxies

Collecting Lots of Free 'Micro-Deposits'

Using your browser URL history to estimate gender

Cross-site File Upload Attacks

Same Origin Bypassing Using Image Dimensions

HTTP Proxies Bypass Firewalls

Join a Religion Via CSRF

Cross-domain leaks of site logins via

Authenticated CSS

JavaScript Global Namespace Pollution

GIFAR

HTML/CSS Injections - Primitive Malicious Code

Hacking Intranets Through Web Interfaces

Cookie Path Traversal

Racing to downgrade users to cookie-less

authentication

MySQL and SQL Column Truncation Vulnerabilities

Building Subversive File Sharing With Client

Side Applications

Firefox XML injection into parse of remote XML

# New web hacking techniques

Firefox cross-domain information theft	Pulling system32 out over blind SQL Injection
(simple text strings, some CSV)	Dialog Spoofing - Firefox Basic Authentication
Firefox 2 and WebKit nightly cross-domain image theft	Skype cross-zone scripting vulnerability
Browser's Ghost Busters	Safari pwns Internet Explorer
Exploiting XSS vulnerabilities on cookies	IE "Print Table of Links" Cross-Zone Scripting Vulnerability
Breaking Google Gears' Cross-Origin Communication Model	A different Opera
Flash Parameter Injection	Abusing HTML 5 Structured Client-side Storage
Cross Environment Hopping	SSID Script Injection
Exploiting Logged Out XSS Vulnerabilities	DHCP Script Injection
Exploiting CSRF Protected XSS	File Download Injection
ActiveX Repurposing	Navigation Hijacking (Frame/Tab Injection Attacks)
Tunneling tcp over http over sql-injection	UPnP Hacking via Flash
Arbitrary TCP over uploaded pages	Total surveillance made easy with VoIP phone
Local DoS on CUPS to a remote exploit via specially-crafted webpage	Social Networks Evil Twin Attacks
JavaScript Code Flow Manipulation	Recursive File Include DoS
Common localhost dns misconfiguration can lead to "same site" scripting	

# New web hacking techniques

Multi-pass filters bypass

Session Extending

Code Execution via XSS

Redirector's hell

Persistent SQL Injection

JSON Hijacking with UTF-7

SQL Smuggling

Abusing PHP Sockets

CSRF on Novell GroupWise WebAccess

# Top Ten Web Hacking Techniques (2008)

- Flash Parameter Injection
- ActiveX Repurposing
- Tunneling TCP over HTTP over SQL-Injection
- Cross-domain leaks of site logins via Authenticated CSS
- Abusing HTML 5 Structured Client-side Storage
- A Different Opera
- Clickjacking / Videojacking
- Safari Carpet Bomb
- Breaking Google Gears' Cross-Origin Communication Model
- GIFAR

# Goals of attacks

- Defacing
- Data theft
- Ideological hacking
- Stealing sensitive information
- Planting malware
- Causing monetary loss

# Questions

- Can we have enough number of qualified web programmers? No
- Is the certification a panacea against low quality web sites? No
- Can we have enough number of certified web application security specialists? No
- Can an auditing mechanism be introduced before launching the web site? No

# Questions

- Can a hosting company have a very qualified web application security specialist? Yes
- Can it be achieved that all new web sites are hosted on a hosting company server?  
Yes, web outsourcing is more effective and less expensive.
- Can a hosting company perform an audit of the web site before hosting? Yes

# Questions

- Can sysadmin effectively perform the job of information security officer? No, information security is a profession and not an additional headache to system administrators.
- Is there a need in information security officer in an average size company / organization? Yes.
- Will a company/organization introduce a position of information security officer? No

# Conclusion

- Outsourcing of web sites and other security services is the best solution.

# Recommendations

- Obligate governmental and educational organizations to use licensed antivirus software with automated updates from network servers. Insist on using the software update service.
- Obligate systems administrators/security officers to report each attack on their network to the national security center (CERT AM)
- Expand system administrators' participation in CERT.AM operations
- Introduce Cyber Storm type national exercises to check the country preparedness for cyber attacks

# Recommendations

- Recommend hosting companies to introduce the position of information security officers
- Recommend hosting companies to audit the security of the hosted web sites
- Recommend companies developing their web sites to order it from web site development companies well known in the market
- Require information security certification from the applicant to the position of information security officer
- Organize training of certified security officers in Armenia

Internet is facing a great danger - the whole  
DNS system is under attack.

It is a matter of primary importance to  
ensure DNS system stability and security.

The danger is Conficker worm.

Now some slides from John Crain's presentation "ccTLD security issues, attacks, conficker"

John Crain is Senior Director,  
Security, Stability and Resiliency Programs  
ICANN ([john.crain@icann.org](mailto:john.crain@icann.org))

# What is Conficker?

- An Internet worm
  - Self-replicating malicious code
  - Uses a network for distribution
- Uses various methods to spread the infection (network file shares, map drives, removable media)
- Conficker code is *injected* into Windows Server Service
  - Variants disable security measures
  - Provides the attacker with remote control, execution privileges, and ability to download more malware
- Enlists the infected computer into a botnet
  - Conficker bots query rendezvous points for additional malware or instructions for already present malware

## **Fighting Conficker: Chronology of Events**

- November 2008 – 1 January 2009
  - Security community identify Conficker.A
  - Researchers register domains to contain botnet
- 2 January – 3 February 2009
  - Conficker.B name algorithm uses more names, more TLDs
  - Security community asks DNS community for help in containing  
Conficker
    - DNS community joins ad hoc partnership, blocks Conficker domains at registry
- 12 February 2009
  - Public announcement of collaborative operational response
  - Microsoft offers \$250,000 reward

## **Fighting Conficker:**

### **Chronology of Events (Cont'd)**

- 19 February 2009 – 31 March 2009
  - Conficker.C/D identified, more aggressive in domain registrations, begins using P2P
  - DNS community continues to block domains, Security community releases Conficker scanners
- 1 April 2009
  - Conficker.E variant activated on previously infected hosts
- 3 May 2009 - present
  - Conficker.E variant removes itself but leaves DLL and P2P network in place
  - Security community continues to monitor activities and collaborate on keeping blocks in place

## Problems not yet solved

- Collaborative response forced botnet operators out of comfort zone but not out of business
- Botnet writers are agile and elusive
  - Cannot put them out of business without adopting a similarly agile model for response
- Collaboration can be difficult to sustain
  - Numerous and complex, harder to build and maintain, more fragile than botnets
- The risk-reward equation favors worm creators

# What do these incidents reveal? (from SAC040 study)

- All an attacker needs to gain control of an entire domain name portfolio is a user account and password
  - Guess, phish, or socially engineer a single point of contact
  - Attackers also scan registrar account login portals for web application vulnerabilities
  - Attacker can change contact and DNS information of **ALL** domains in the account
- Email may be only method registrar employs to notify a registrant
  - of account activity
  - Attackers know this and block delivery to registrant by altering DNS configuration
- Recovery from DNS configuration abuse is slow

## Findings (from SAC040 study)

- Attackers exploit password-based authentication to gain access registration accounts
  - Compromise exposes all domains in account to attack
  - DNS configurations are favorite targets
- Attackers often alter DNS configurations to prevent email delivery of registrar notifications to registrants
- Security measures vary among registrars
  - Customers need more information to make informed decisions when choosing a registrar
- Domain name account access should be as secure as an ebanking or e-merchant transaction

# Recommendations (from SAC040 study)

- Registrars: offer more protection against registration exploitation or misuse
  - Complement existing measures to protect domain accounts with security measures identified in the SSAC report
- Registrars: make information describing measures to protect domain accounts more accessible to customers
- Registrars: consider a voluntary, independent security audit as a component of self-imposed security due diligence
- ICANN: consider whether a trusted security mark programs would improve registration services security