

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1211

(09/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Techniques for preventing web-based attacks

Recommendation ITU-T X.1211

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1211

Techniques for preventing web-based attacks

Summary

Recommendation ITU-T X.1211 describes techniques that can mitigate web-based attacks which occur when the vulnerabilities of the website hosts are exploited and malicious code is introduced that can infect a user's computer. Several appendices illustrate how the attacks can occur as well as remediation steps.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1211	2014-09-26	17	11.1002/1000/12154

Keywords

Prevention, SQL injection, spyware, suspicious content, vulnerability, web-based attack.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2014

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Terms and definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 General overview.....	3
7 Web-based attack protection system techniques	4
7.1 General techniques	4
7.2 Functional techniques.....	4
7.3 Management techniques	5
7.4 Security and privacy techniques.....	5
8 Functions of the web-based attack protection system	5
9 Information exchange format	6
Appendix I – Scenarios for web-based attacks	7
I.1 Scenario for malware infection	7
I.2 Cross-site request forgery (CAPEC-62).....	7
I.3 Cross-site port attacks/server-side request forgery.....	8
I.4 SQL injection.....	8
I.5 Detecting malware in websites.....	9
Appendix II – Method for infecting user computers with malware.....	10
Appendix III – Typical examples of obfuscation technique	11
Appendix IV – Prevention techniques for web-based attacks	12
IV.1 Remove website vulnerabilities.....	12
IV.2 Signature matching.....	12
IV.3 Site blacklisting	12
IV.4 Detection of obfuscating techniques	12
IV.5 Evaluation of suspicious content behaviour	12
Appendix V – Typical examples of application security risks by OWASP	13
Bibliography.....	22

.....

Recommendation ITU-T X.1211

Techniques for preventing web-based attacks

1 Scope

This Recommendation provides techniques for preventing web-based attacks. It describes the use scenarios to distributing malwares through the web as well as the functional techniques and functions to prevent web-based attacks.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 asset [b-ISO/IEC 27000]: Anything that has value to the organization.

NOTE – There are many types of assets, including:

- a) information;
- b) software, such as a computer program;
- c) physical, such as computer;
- d) services;
- e) people, and their qualifications, skills, and experience; and
- f) intangibles, such as reputation and image.

3.1.2 attack instance [b-ITU-T X.1544]: A specific detailed attack against an application or system targeting vulnerabilities or weaknesses in that system.

3.1.3 attack pattern [b-ITU-T X.1544]: An abstraction of common approaches of attack observed in the wild against applications or systems (e.g., SQL injection, man-in-the-middle, session hijacking).

NOTE – A single attack pattern may potentially have many varying attack instances associable with it.

3.1.4 hypertext markup language (HTML) [b-ITU-T M.3030]: A system of coding information from a wide range of domains (e.g., text, graphics, database query results) for display by World Wide Web browsers. Certain special codes, called tags, are embedded in the document so that the browser can be told how to render the information.

3.1.5 malware [b-ISO/IEC 27033-1]: Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

3.1.6 obfuscation technique [b-NIST SP 800-83]: A way of constructing a virus to make it more difficult to detect.

3.1.7 personally identifiable information (PII) [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.1.8 threat [b-ITU-T X.800]: A potential violation of security.

3.1.9 security domain [b-ITU-T T.411]: The set of resources subject to a single security policy.



3.1.10 security domain authority [b-ITU-T X.810]: A security authority that is responsible for the implementation of a security policy for a security domain.

3.1.11 security policy [b-ITU-T T.411]: The set of rules that specify the procedures and services required to maintain the intended level of security of a set of resources.

3.1.12 signature [b-NIST SP 800-83]: A set of characteristics of known malware instances that can be used to identify known malware and some new variants of known malware.

3.1.13 spyware [b-NIST SP 800-83]: Malware intended to violate a user's privacy.

3.1.14 web browser plug-in [b-NIST SP 800-83]: A mechanism for displaying or executing certain types of content through a Web browser.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 anomaly: A pattern in the data that does not conform to the expected behaviour.

3.2.2 drive-by-download attacks: A pattern of a web-based attack caused when a user visits a website that exploits browser vulnerabilities and launches the automatic download and installation of malware without the knowledge or permission of the user.

3.2.3 web-based attack: A pattern of attacks in which the attackers compromise the legitimate websites resulting in a malicious code to be injected into an application, which in turn can be used to infect the user's computer visiting those websites or use vulnerabilities of web sites to launch attacks for user's computer systems that visit that web sites, which occurs without involvement of malware.

3.2.4 web-based attack protection system: A set of systems which detects vulnerabilities, malwares or malicious codes embedded in the legitimate website and informs the web administrator of the detection result, leading ultimately to their removal.

NOTE – Detection activities may be planned by schedule or may be triggered by network events or requests from other systems.

3.2.5 zombie computer: A computer that has been compromised and controlled by an attacker who has installed malwares such as computer viruses, Trojan horse, or bot net, which can be used to perform malicious attacks such as spreading e-mail spams and launching denial-of-service attacks.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAPEC	Common Attack Pattern Enumeration and Classification
CSRF	Cross-Site Request Forgery
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DOM	Document Object Model
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ID	Identity
IODEF	Incident Object Description Exchange Format
LDAP	Lightweight Directory Access Protocol

MITM	Man-in-the-Middle
OS	Operating System
OWASP	Open Web Applications Security Project
PC	Personal Computer
PII	Personally Identifiable Information
PUI	Program Under Inspection
SNS	Social Network Service
SQL	Structured Query Language
SSRF	Server-Side Request Forgery
S/W	Software
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XSPA	Cross-Site Port Attack
XSS	Cross-Site Scripting

5 Conventions

None.

6 General overview

Malware that is used to compromise information assets is defined as software designed specifically to damage or to disrupt a system, attacking confidentiality, integrity and/or availability. It includes computer viruses, worms, Trojan horses, spyware, adware, most rootkits and other malicious programs.

A web-based attack is an attack whereby the attackers try to compromise the legitimate websites by exploiting existing vulnerabilities. This results in malicious code to be injected into the websites, which can in turn be used to infect the computers of users visiting those websites. The malicious code may have multiple forms: it can be a hidden iframe tag directing the user to visit an attack site, or it can be malicious applications written in a computer program language (e.g., script or applets). Typical examples of vulnerabilities of web-based attacks are Structured Query Language (SQL) injection, and cross-site request forgery (CSRF).

A cross-site request forgery attack pattern [b-CAPEC-62] is a type of web-based attack whereby unauthorized commands are transmitted or unwanted actions are requested to be executed on a trusted website without the user's knowledge while the user is logged into a trusted website. A Structured Query Language (SQL) injection attack pattern [b-CAPEC-66] is another type of web-based attack on a database-driven website in which the attacker adds an SQL code to a web form from an input box to gain access to resources or make changes to data. It is used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database. An in-line frame, also known as iframe tag [b-iframe], is used to embed an invisible document within the current hypertext markup language (HTML) document and tricking the user to click on the invisible document through clickjacking [b-CAPEC-103].

Recently, web-based attacks have been increasing significantly due to increasing use of end-user computing devices and the increasing number of websites that contain malware.

Anti-virus techniques could be implemented at the server side and web application firewalls could be implemented at proxies for cost-effective implementation of these techniques.

In web-based attacks, the administrators of the websites may not be aware that the websites have been hacked and injected with malicious code, and that these are used to disseminate malicious code. Moreover, users are not aware either that their computers may get infected by malicious code from the sites they have visited. Installing anti-virus software (S/W) can prevent some incidents, but does not provide ultimate solutions.

The reasons for an increase in web-based attacks are as follows:

- Drive-by-download attacks from mainstream web sites are increasing;
- Attacks are heavily obfuscated and dynamically changing, making traditional malware detection and prevention solutions ineffective;
- Attacks are targeting web browser plug-ins of end users;
- SQL injection attacks are being used to infect mainstream websites;
- Malicious advertisements are redirecting users to malicious websites; and
- An explosive growth in unique and targeted malware samples.

7 Web-based attack protection system techniques

7.1 General techniques

The following techniques are characteristic of the web-based attack protection system:

- designed to be scalable, robust and resilient;
- operated across multiple security domains, each of which is managed by a responsible security administrator; and
- exchange information about website vulnerabilities or malware-infected websites (i.e., websites with invisible iframe redirecting users to the malware-infected website [b-CAPEC-103]);

NOTE – The existing incident object description exchange format (IODEF) [b-ITU-T X.1541] could be used to exchange information.

- operated in one of the two types of deployment models: a centralized model and a distributed model. In the centralized model, all information about the malware-infected websites and types of malware should be reported to, maintained or controlled by the centralized server. In the distributed model, each security domain should set up a responsible agent and information about the malware-infected websites and types of malware should be exchanged among the responsible agents that exist in distributed locations;
- configured in a hierarchical manner to facilitate the scalable operation.

7.2 Functional techniques

The following functional techniques are characteristic of the web-based attack protection system:

- identify known malware from legitimate web content and prevent websites from the malware being installed;
- detect the invisible iframe that redirects the user to other websites that install malware;
- detect vulnerabilities that can be used for typical web-based attacks such as SQL injection, cross-site reference, etc., as described in Appendix IV;
- conduct signature-based analysis or equivalent analysis to detect the known malware in the website;