ITU-T CYBEX standards for cybersecurity information dissemination and exchange

ITU-ATU Workshop on Cybersecurity Security Strategy in African Countries
Session 4: National versus regional versus international

Martin Euchner
Adviser, ITU-T

Khartoum, Sudan, 24-26 July 2016

(See notes pages for more information)
Contents

- ITU-T Study Group 17, and Question 4/17, Cybersecurity
- Cyberspace security, ITU-T definition of Cybersecurity

- Knowledge-based standards for CYbersecurity Information eXchange (CYBEX) (ITU-T X.1500-series Recommendations)
  - CVE: Common Vulnerability Enumeration
  - CVSS: Common Vulnerability Scoring System (3.0)
  - Common Weakness Enumeration (CWE)
  - Common weakness scoring system (CWSS)
  - Language for the open definition of vulnerabilities and for the assessment of a system state (OVAL)
  - Discovery mechanisms in the exchange of cybersecurity information
  - Incident object description exchange format (IODEF)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Malware attribute enumeration and classification (MAEC)
ITU-T Study Group 17 mandate

- Title: Security

Responsible for building confidence and security in the use of information and communication technologies (ICTs).

This includes studies relating to cybersecurity, security management, countering spam and identity management.

It also includes security architecture and framework, protection of personally identifiable information, and security of applications and services for the Internet of things, smart grid, smartphone, IPTV, web services, social network, cloud computing, mobile financial system and telebiometrics.

Also responsible for the application of open system communications including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, and for conformance testing to improve quality of Recommendations.

Chairman: Arkadiy Kremer, Russian Federation
Cybersecurity by design no longer possible; a new paradigm:
  • know your weaknesses → minimize the vulnerabilities
  • know your attacks → share the heuristics within trust communities

Current work program (6 Recommendations under development)
  X.1500 suite: Cybersecurity Information Exchange (CYBEX) – non-prescriptive, extensible, complementary techniques for the new paradigm
    • Weakness, vulnerability and state
    • Event, incident, and heuristics
    • Information exchange policy
    • Identification, discovery, and query
    • Identity assurance
    • Exchange protocols
  Non-CYBEX deliverables include compendiums and guidelines for
    • Abnormal traffic detection
    • Botnet mitigation
    • Attack source attribution (including traceback)

Extensive relationships with many external bodies
Rapporteur: Mr Youki KADOBAYASHI
Definition of Cybersecurity

Definition of Cybersecurity
(ref. Rec. ITU-T X.1205, Overview of cybersecurity):
Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.
Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment.
The general security objectives comprise the following:

– Availability

– Integrity, which may include authenticity and non-repudiation

– Confidentiality.
Capacity building with ITU-T cybersecurity standards

- Existing process-oriented standards, as well as checklist standards, should be complemented with detailed knowledge-base of cybersecurity, because:
  - Cyber-risks are highly volatile
  - Chain reactions are typical
difficult to estimate the risk without considering technical detail
  - You’ll need to communicate the detail

- ITU-T provides knowledge-base standards.
Improving cybersecurity throughout IT infrastructure lifecycle

Development
- CWE X.1524
- CAPEC X.1544

Deployment
- CVE X.1520
- CVSS X.1521

Assessment
- OVAL X.1526
- CPE X.1528

Knowledge bases, compatible products, informed communities and ITU-T Recommendations are already helping diverse organizations to protect their IT infrastructures and customers.
Examples of CYBEX usage

- **National coordination centers for cybersecurity** make use of vulnerability information identifiers and scoring standards for public alerting purposes.

- **Incident response teams** efficiently keep track of vulnerabilities and attack patterns through a set of concise identifiers as predicated by CYBEX.

- **System administrators** assess presence of vulnerabilities using software tools that employ CYBEX.

- **Cloud computing and network service providers** keep track of vulnerabilities in their infrastructure, where they are prioritized according to impact, using the standardized scoring method.

- **Embedded and IoT product developers** learn typical patterns of software weaknesses through public knowledge base that is also part of CYBEX.

- **Vulnerability researchers** collectively maintain knowledge bases of vulnerabilities, each of which can be linked and integrated through common vulnerability identifiers.
Cybersecurity Information Exchange (CYBEX)

- Overview of cybersecurity information exchange (Rec. ITU-T X.1500)
- Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange (Rec. ITU-T X.1500.1)

Rec. ITU-T X.1500 - CYBEX model
Knowledge base of vulnerabilities
CVE: Common Vulnerability Enumeration

- A structured means to exchange information on security vulnerabilities and exposures
- Provides a common identifier with status indicator, a brief description and references to related vulnerability report and advisories for publicly-known problems.
- Standardized as **Rec. ITU-T X.1520**
- Applicable to national vulnerability databases:
  - U.S. NIST NVD
  - Japan JVN

- CVE community: [http://cve.mitre.org/](http://cve.mitre.org/)
Example
Vulnerabilities of widely used software for data protection purposes

CVE entries for MySQL

CVE-2014-5139
- Description: DoS
- Publish Date: 2014-08-13
- Update Date: 2014-08-15
- Score: 4.3
- Gained Access Level: None
- Access: Remote
- Complexity: Medium

The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL server applications to trigger a ServerHello message that includes an SRP ciphersuite with an invalid ciphersuite with the client.

CVE-2014-3512 119
- Description: DoS Overflow
- Publish Date: 2014-08-13
- Update Date: 2014-08-14
- Score: 7.5
- Gained Access Level: None
- Access: Remote
- Complexity: Low

Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allows remote SSL server applications to possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameters that are used to perform an SRP handshake.

CVE-2014-3511
- Description: DoS
- Publish Date: 2014-08-13
- Update Date: 2014-08-14
- Score: 4.3
- Gained Access Level: None
- Access: Remote
- Complexity: Medium

The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to trigger ClientHello message fragmentation in communication between a client and server that both support "protocol downgrade" issue.
Ongoing proliferation of CVE

- More than 150 CVE-compatible products and services
Quantification of vulnerabilities facilitates prioritization during vulnerability management

- CVSS: Common Vulnerability Scoring System (3.0)
  - Base metrics: constant over time and across user environments
  - Temporal metrics: reflects vulnerability landscape
  - Environmental metrics: reflects user environments
  - Standardized as Rec. ITU-T X.1521
  - Community: http://www.first.org/cvss/

Rec. ITU-T X.1521 – CVSS metric groups

Rating | CVSS Score
--- | ---
None | 0.0
Low | 0.1 – 3.9
Medium | 4.0 – 6.9
High | 7.0 – 8.9
Critical | 9.0 – 10.0
Taxonomy of vulnerabilities

Common Weakness Enumeration (CWE)

Rec. ITU-T X.1524

- Group same kind of vulnerabilities into a weakness, and give it a distinct number
- Provides common names for publicly known problems in the commercial or open source software
- Intended for security tools and services that can find weaknesses in source code and operational systems
- Helps better understand and manage software weaknesses related to architecture and design
- Community: [http://cwe.mitre.org/](http://cwe.mitre.org/)

<table>
<thead>
<tr>
<th>CWE-89: Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td>Weakness Prevalence</td>
</tr>
<tr>
<td>Remediation Cost</td>
</tr>
<tr>
<td>Attack Frequency</td>
</tr>
</tbody>
</table>

Discussion

These days, it seems as if software is all about the data: getting it into the database, pulling it from the database, massaging it into information, and sending it elsewhere for fun and profit. If attackers can influence the SQL that you use to communicate with your database, then suddenly all your fun and profit belongs to them. If you use SQL queries in security controls such as authentication, attackers could alter the logic of those queries to bypass security. They could modify the queries to steal, corrupt, or otherwise change your underlying data. They’ll even steal data one byte at a time if they have to, and they have the patience and know-how to do so. In 2011, SQL injection was responsible for the compromises of many high-profile organizations, including Sony Pictures, PBS, MySQL.com, security company HBGary Federal, and many others.
### CWE top 25

http://cwe.mitre.org/top25/

- Prioritized list of dangerous software errors
  - Intended to minimize software vulnerability and data breach
  - Any software for data protection needs serious consideration of these failure modes, among others

#### Useful for:
- Procurement
- Development, etc.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Score</th>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>93.8</td>
<td>CWE-89</td>
<td>Improper Neutralization of Special Elements used in an SQL Command</td>
</tr>
<tr>
<td>[2]</td>
<td>83.3</td>
<td>CWE-78</td>
<td>Improper Neutralization of Special Elements used in an OS Command</td>
</tr>
<tr>
<td>[3]</td>
<td>79</td>
<td>CWE-120</td>
<td>Buffer Copy without Checking Size of Input</td>
</tr>
<tr>
<td>[4]</td>
<td>77.7</td>
<td>CWE-79</td>
<td>Improper Neutralization of Input During Web Page Generation</td>
</tr>
<tr>
<td>[6]</td>
<td>76.8</td>
<td>CWE-862</td>
<td>Missing Authorization</td>
</tr>
<tr>
<td>[7]</td>
<td>75</td>
<td>CWE-798</td>
<td>Use of Hard-coded Credentials</td>
</tr>
<tr>
<td>[8]</td>
<td>75</td>
<td>CWE-311</td>
<td>Missing Encryption of Sensitive Data</td>
</tr>
<tr>
<td>[9]</td>
<td>74</td>
<td>CWE-434</td>
<td>Unrestricted Upload of File with Dangerous Type</td>
</tr>
<tr>
<td>[10]</td>
<td>73.8</td>
<td>CWE-807</td>
<td>Reliance on Untrusted Inputs in a Security Decision</td>
</tr>
<tr>
<td>[11]</td>
<td>73.1</td>
<td>CWE-250</td>
<td>Execution with Unnecessary Privileges</td>
</tr>
<tr>
<td>[12]</td>
<td>70.1</td>
<td>CWE-352</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>[13]</td>
<td>69.3</td>
<td>CWE-22</td>
<td>Improper Limitation of a Pathname to a Restricted Directory</td>
</tr>
<tr>
<td>[14]</td>
<td>68.5</td>
<td>CWE-494</td>
<td>Download of Code Without Integrity Check</td>
</tr>
<tr>
<td>[16]</td>
<td>66</td>
<td>CWE-829</td>
<td>Inclusion of Functionality from Untrusted Control Sphere</td>
</tr>
<tr>
<td>[17]</td>
<td>65.5</td>
<td>CWE-732</td>
<td>Incorrect Permission Assignment for Critical Resource</td>
</tr>
<tr>
<td>[18]</td>
<td>64.6</td>
<td>CWE-676</td>
<td>Use of Potentially Dangerous Function</td>
</tr>
<tr>
<td>[19]</td>
<td>64.1</td>
<td>CWE-327</td>
<td>Use of a Broken or Risky Cryptographic Algorithm</td>
</tr>
<tr>
<td>[20]</td>
<td>62.4</td>
<td>CWE-131</td>
<td>Incorrect Calculation of Buffer Size</td>
</tr>
<tr>
<td>[21]</td>
<td>61.5</td>
<td>CWE-307</td>
<td>Improper Restriction of Excessive Authentication Attempts</td>
</tr>
<tr>
<td>[22]</td>
<td>61.1</td>
<td>CWE-601</td>
<td>URL Redirection to Untrusted Site</td>
</tr>
<tr>
<td>[23]</td>
<td>61</td>
<td>CWE-134</td>
<td>Uncontrolled Format String</td>
</tr>
<tr>
<td>[24]</td>
<td>60.3</td>
<td>CWE-190</td>
<td>Integer Overflow or Wraparound</td>
</tr>
<tr>
<td>[25]</td>
<td>59.9</td>
<td>CWE-759</td>
<td>Use of a One-Way Hash without a Salt</td>
</tr>
</tbody>
</table>

- Prioritized list of dangerous software errors
  - Intended to minimize software vulnerability and data breach
  - Any software for data protection needs serious consideration of these failure modes, among others

- Useful for:
  - Procurement
  - Development, etc.
Common weakness scoring system (CWSS) (Rec. ITU-T X.1525)
Vulnerability assessment

- Language for the open definition of vulnerabilities and for the assessment of a system state (OVAL) (Rec. ITU-T X.1526)
  - A standard for assessment and reporting of machine state of computer systems; such as vulnerability state, patch state, configuration state.
  - OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.
  - Community: [http://oval.mitre.org/](http://oval.mitre.org/)

- Common platform enumeration (CPE)
  (Recs. ITU-T X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4)

---

Search Results (Refine Search)
There are 1 matching records.

cpe:2.3:a:$/0.99_kindle_books_project/$0.99_kindle_books:6:*:*:*:*:android:*:*
Vendor: $0.99_kindle_books_project
Product: $0.99_kindle_books
Version: 6
View CVEs
CYBEX identification and discovery

- Discovery mechanisms in the exchange of cybersecurity information (Rec. ITU-T X.1570)

Rec. ITU-T X.1570 - Cybersecurity operational information ontology
CYBEX event/incident/heuristics exchange

- Incident object description exchange format (IODEF) ([Rec. ITU-T X.1541](https://www.itu.int/rec/T-REC-X.1541)) describes the information model for IODEF format (IETF RFC 5070) and provides an associated data model specified with XML schema. IODEF specifies a data model representation for sharing commonly exchanged information about computer security or other incident types.
- IODEF enhances operational capabilities and improves situational awareness.

- The IODEF structured format (in XML Schema) allows for:
  - increased automation in the processing of incident information through the exchange of structured incident information, eliminating the need for security analysts to parse free-form textual documents;
  - decreased effort in correlating similar data (even when highly structured) from different sources enhancing situational awareness;
  - a common format on which to provide interoperability between tools for incident handling and analysis, specifically when information comes from multiple entities.
Knowledge base of attack patterns

- Common Attack Pattern Enumeration and Classification (CAPEC) (Rec. ITU-T X.1544)
  - Dictionary of attack patterns, solutions & mitigations
  - Facilitates communication of incidents, issues, as well as validation techniques and mitigation strategies
  - Community: http://capec.mitre.org/

CAPEC example: SQL injection

CAPEC-66: SQL Injection

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This attack exploits target software that constructs SQL statements based on user input, then input strings so that when the target software constructs SQL statements based on these strings, the statement performs actions other than those the application intended. SQL Injection results from failure of the application to appropriately validate input. When untrusted user input consisting of SQL syntax is used without proper validation as part of SQL statement construction, the attacker can exploit the database in ways not envisaged during application design. SQL Injection can be leveraged to execute system-related commands of the attacker’s choice. SQL Injection enables an attacker to execute arbitrary SQL statements in the database, thus bypassing the application completely. In order to successfully inject content from a database, an attacker:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Methods of Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Injection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples-Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
</tr>
<tr>
<td>With PHP-Nuke versions 7.9 and earlier, an attacker can successfully access and modify data, including sensitive contents such as usernames and password hashes, and compromise the application through SQL injection. The protection mechanism against SQL injection employs a blacklist approach to input validation. However, because of improper blacklisting, it is possible to inject content such as &quot;foo/+++UNION&quot; or &quot;foo UNION/*&quot; to bypass validation and glean sensitive information from the database.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-5525</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attacker Skills or Knowledge Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill or Knowledge Level: Low</td>
</tr>
<tr>
<td>It is fairly simple for someone with basic SQL knowledge to perform SQL injection, in general. In certain instances, however, specific knowledge of the database employed may be required.</td>
</tr>
</tbody>
</table>
Malware attribute enumeration and classification (MAEC) (Rec. ITU-T X.1546)
CYBEX assured exchange

- Real-time inter-network defence (RID) ([Rec. ITU-T X.1580](https://www.itu.int/rec/T-REC-X.1580)): RID specifies a method to securely communicate incident information, enabling the exchange of IODEF XML documents.
  - RID conveys security, policy, and privacy controls to enable the exchange of potentially sensitive information.
  - RID includes provisions for secrecy, confidentiality, integrity and authentication for the exchange of incident information.

- Transport of real-time inter-network defence messages ([Rec. ITU-T X.1581](https://www.itu.int/rec/T-REC-X.1581)) (IETF RFC 6546):
  - Specifies a transport protocol for RID messages over HTTP/TLS.

- Transport protocols supporting cybersecurity information exchange ([Rec. ITU-T X.1582](https://www.itu.int/rec/T-REC-X.1582))
Summary

- ITU-T Study Group 17 developed international standards on security and on cybersecurity
  - The ITU-T X.1500-series of Recommendations on cybersecurity information exchange (CYBEX) provide critical instruments to deal with rapidly changing and diversifying cybersecurity phenomena, directly contributing to data protection
  - Enumeration standards provide effective means of communication across businesses, government agencies as well as communities
  - Cyber-risks are highly volatile and manifest through unexpected combination of components, that require careful examination of technical risks through knowledge-base standards.
Thank you very much for your attention!
Slides, abstracts, biographies of joint ITU/ATU Workshop on "Cybersecurity strategy in African countries“ freely available on ITU-T web-page at

http://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Pages/Programme.aspx
Backup
Question 4/17
Cybersecurity

- Recommendation in TAP approval process
  - X.1542 (X.simef), Session information message exchange format

- Recommendations on CYBEX currently under study include:
  - X.1500 Amd.10, Overview of cybersecurity information exchange – Amendment 10 - Revised structured cybersecurity information exchange techniques
  - X.nessa, Access control models for incidents exchange networks

- Recommendations (non-CYBEX) currently under study include:
  - X.cogent, Design considerations for improved end-user perception of trustworthiness indicators
  - X.metric, Metrics for evaluating threat and resilience in cyberspace
  - X.samtn, Security assessment techniques in telecommunication/ICT networks
  - X.sbb, Security capability requirements for countering smartphone-based botnets

In this study period, Q4/17 has developed eight new Recommendations (X.1208, X.1210, X.1211, X.1303bis, X.1525, X.1544, X.1546, X.1582), 3 revised Recommendations (X.1520, X.1521, X.1526), seven new Amendments (X.1500 Amds.3-9), 2 new supplements (X.Suppl.18, X.Suppl.20), and 1 revised supplement (X.Suppl.10).
CYBERSPACE SECURITY – Cybersecurity

- Overview of cybersecurity (Rec. ITU-T X.1205)
- A vendor-neutral framework for automatic notification of security related information and dissemination of updates (Rec. ITU-T X.1206)
- Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software (Rec. ITU-T X.1207)
- A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies (Rec. ITU-T X.1208)
- Capabilities and their context scenarios for cybersecurity information sharing and exchange (Rec. ITU-T X.1209)
- Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks (Rec. ITU-T X.1210)
- Techniques for preventing web-based attacks (Rec. ITU-T X.1211)
Reference links

- Webpage for ITU-T Study Group 17
  - [http://itu.int/ITU-T/studygroups/com17](http://itu.int/ITU-T/studygroups/com17)

- Webpage on ICT security standard roadmap

- Webpage for JCA on child online protection

- Webpage for JCA on identity management

- Webpage on lead study group on security

- Webpage on lead study group on identity management