国　际　电　信　联　盟

ITU-T X.1235

(01/2022)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 打击垃圾信息

电信组织用于对抗网站欺诈的技术

ITU-T X.1235建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	**X.1230–X.1249**
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1235建议书

电信组织用于对抗网站欺诈的技术

摘要

网站欺诈是电信组织、尤其是运营商面临的主要威胁。建议电信运营商采用反网站欺诈技术来保护其客户、保护其声誉和收益。ITU-T X.1235建议书分析了欺诈网站的主要手段，并推荐了用于确定被欺诈网站的技术，可作为电信组织保护网站免受欺诈的导则。可以实施类似的方法来防止欺诈任何网站，包括银行、保险公司、互联网商店等的网站。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1235	2022-01-07	17	11.1002/1000/14797

关键词

应对措施，网站欺诈。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联没有收到实施本建议书可能需要的受专利/软件版权保护的知识产权通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询可通过ITU-T网站获得的适当的ITU-T数据库，网址为：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2022

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

引言

近年来，网络欺诈在互联网欺诈中扮演着主要角色。欺诈者通常选择知名组织或公司的网站来收集访问者的证书或传播恶意软件。这导致访问者和电信运营商的经济损失，以及电信运营商的声誉损失。

由于电信运营商的网站已成为其客户查询和订购各种各样服务的最重要门户之一，因此从世界范围内来看，欺诈者会不断尝试伪造电信运营商的网站，目标是欺诈客户。本建议书对网站欺诈做了全面分析，并提出了一系列有组织的对抗措施。

ITU-T X.1235建议书

电信组织用于对抗网站欺诈的技术

1 范围

本建议书为电信组织提供了关于及时确定网站欺诈并保护其网站免受欺诈的技术的建议。在对欺诈手段和特征进行系统分析后，提供了关于在用户侧技术辅助下应用网络侧技术对抗网站欺诈的最佳做法的建议。

遵循本建议书并不意味着就可证明符合任何国家或地区法律、法规或政策的要求。本建议书中所述的技术方法、组织方式和程序手段并不能以任何形式保证可以达成某种等级的安全性，而使特定的国家或地区法律、法规或政策将之用于某种通信中。

可以实施类似的方法来防止欺诈任何网站，包括银行、保险公司、互联网商店等的网站。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 定义

3.1 他处定义的术语

无。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 卷积神经网络（convolutional neural network）：一种深度学习算法，它接受输入图像，为图像中的各个方面/对象指配重要性，并能将之一一区分开来。

3.2.2 长短期记忆网络（long short-term memory networks）：一种循环神经网络，它能够学习序列预测问题中的顺序依赖性。

3.2.3 循环神经网络（recurrent neural network）：一类神经网络，它允许将先前的输出用作输入，同时具有隐藏状态。

3.2.4 尺度不变特征变换（scale-invariant feature transform（SIFT））：计算机视觉中的一种特征检测算法，用于检测和描述图像中的局部特征，它构成对图像域中平移、旋转和尺度变换不变的描述性标识符，并对适度的视角变换和亮度变化具有鲁棒性。实验证明，SIFT描述性标识符在现实世界条件下的图像匹配和对象识别实践中非常有用。

3.2.5 加速鲁棒特征（speeded up robust features）：计算机视觉中的局部特征检测器和描述性标识符，用于检测和描述图像中的局部特征，它比尺度不变特征变换（SIFT）要快好几倍，并且对不同的图像变换，比SIFT更加鲁棒。

3.2.6 欺诈网站（spoofed website）：通过网站欺诈创建的网站（见第3.2.8节）。

3.2.7 支持向量机（support vector machine）：一种有监督的机器学习模型，用每个类别给定的标记训练数据集来解决两组分类问题，它们能够对新集进行分类。

3.2.8 网站欺诈（website spoofing）：这指的是一系列恶意行为，以模仿为公众或一群人所熟知的网站；而后利用虚假的网站来滥用访问者的信任，以达成恶意的/非法的目标，例如，欺诈、侵犯隐私等。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

AI 人工智能

DNS 域名服务

GUI 图形用户界面

LSTM 长短期记忆

OCR 光学字符识别

PII 个人可识别信息

QR 快速响应

SIFT 尺度不变特征变换

SURF 加速鲁棒特征

SVM 支持向量机

URL 统一资源定位器

5 惯例

本建议书使用下列惯例：

关键词“**应该**”（**should**）指的是一项建议性的、并非绝对要求的要求，因此，宣称遵循本建议书时无需提及该项要求。

关键词“**可以**”（**may**）表示允许作为选项但并非建议遵守的要求。

在本建议的正文中，有时会出现“**能/能够**”（**can**）一词，在这种情况下，它们将被解释为“**能/能够**”（**is able to**）。

6 网站欺诈的分析

网站欺诈指的是一系列恶意行为，以模仿为公众或一群人所熟知的网站。欺诈网站收集访问者的证书或传播恶意软件以达成恶意的/非法的目标，例如，欺诈、侵犯隐私等。

网站欺诈可能会以多种方式造成严重损害。例如，它可能会给客户和运营商带来经济损失、损害运营商的声誉等。此外，即使欺诈网站消失，被泄露的用户信息也可能还会被长期滥用。因此，对电信组织、尤其是运营商而言，采用有用的技术来对抗网站欺诈情况是很重要的。

6.1 网站欺诈场景

创建欺诈网站以实现不正当目标的典型场景包括三个阶段，如图6-1所示。

– **第一阶段：**创建网站
  - 第一步：开发和运营一个与某些知名网站相同或相似的欺诈网站。

– **第二阶段：**传播统一资源定位器（URL）
  - 第二步：通过诸如电子邮件、短信服务、即时通讯服务等各种方法来传播欺诈网站。

– **第三阶段：**收集证书或传播恶意软件
  - 第三步：诱骗访问者输入证书或下载恶意软件。一旦受害者访问了一个欺诈网站，他们就可能会错误地认为该网站是真实的，并使用其证书登录或下载恶意软件。
  - 第四步：检索访问者的证书，并准备下一个骗局或其他恶意活动。

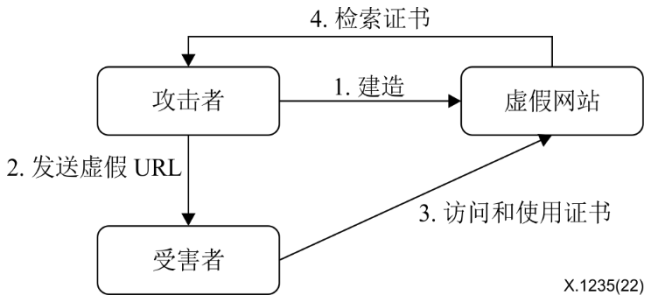


图6-1 – 使用欺诈网站收集用户证书的四个阶段

6.2 网站欺诈的特性

6.2.1 欺诈网站的特性

欺诈网站使用相似技术来欺诈访问者认为他们正在访问真实的网站。它们有若干共同的特性：

– 视觉相似度：欺诈网站可能是真实网站的一个完整副本，包括其视觉内容和交互逻辑。

– 借用视觉元素：欺诈网站可能会从真实网站中借用一些重要的视觉元素。

– 链接知名网站：欺诈网站可能包含至其他知名网站的链接，以模仿授权的合作伙伴网站、相关网站或网站的不同版本。

– 相似域名：欺诈网站的域名会与真实网站的域名非常相似。

– 模糊域名：有时攻击者会使用URL缩短服务或快速响应（QR）码来掩盖网站的真实域名作为一个共享链接。

– 重复域名：一组域名可能会被保留给一个欺诈网站，为了延长欺诈网站的生命周期，其中一些域名将被一次性发布。
– 混淆源代码：欺诈网站的源代码可能会被混淆，以扰乱安全扫描程序。
– 证书输入：欺诈网站可能会引诱访问者输入证书。
– 重定向到已知网站：欺诈网站可能会在空闲时间重定向到已知网站（例如，google.com），以避免自动在线欺诈扫描。
– 虚假地址栏：一些欺诈网站可能是专门为移动网络浏览器设计的。网站可能会在手机屏幕顶部放置一个移动浏览器地址栏的伪造副本，并通过滥用移动浏览器的图形用户界面（GUI）功能来锁定副本。

6.2.2 相关活动的特性

为了引诱或欺诈人们访问欺诈网站并与之互动，可以采取许多活动。这些活动的特性或策略可能是此处列出的一项或多项：

– 传播信息，让尽可能多的人知道欺诈网站的存在。
– 劫持或毒害域名服务（DNS）。因此，对真正网站的任何访问都将被重定向到欺诈网站。
– 利用好处（例如，优惠券和礼物等）诱使用户点击虚假网站链接。
– 在受害者的手机上安装恶意软件，用虚假的请求代替真实的网站请求。
– 模仿客服联系用户，并提供虚假网站链接。

6.3 后果

欺诈网站可对用户和网站所有者产生诸多负面影响。可能的后果如下所述：

– 用户财产损失：用户证书和个人可识别信息（PII）可能被泄露。诈骗者可能会使用该信息来做进一步欺诈。用户可能会被诱骗下载木马、加密挖掘代码和其他恶意软件。用户的终端可能会被控制，以窃取金融账户、传播垃圾邮件和感染其他用户。这些活动会导致电池丢失或终端故障，还会造成直接的和巨大的财务损失。
– 运营商财产损失：用户与运营商之间的正常交易会丢失，甚至长期受到制约。
– 声誉损失：真实网站的声誉甚至运营商的公信力都会受到损害，将会造成大量的客户投诉和长期的负面评价。

7 对策

对抗欺诈网站可分为识别和保护两个方面。前者指的是其他网站中确定欺诈网站，见第7.1节。后者指的是保护用户免于访问已知的欺诈网站或被其欺诈，见第7.2节。

电信组织不必同时使用本节建议的所有技术。由于获取的数据、立法环境和用户要求等，电信组织应灵活采用本节中所述的适当技术。

7.1 识别

根据第6.2.1节中所述的确定的欺诈网站的特性，建议考虑以下对策：

7.1.1 相似域名比较

建议运营商维护一个易被欺诈的知名网站的域名清单。如果域名与清单中的域名非常相似（但不相同），那么它可能是一个欺诈网站的域名。如果域名已被URL短服务缩短，那么应该在比较之前将其转换回初始的URL。

关于两个域名的相似度计算，有许多方法，包括：编辑距离法、Jaccard相似度法、最长公共子序列法、视觉相似度转换法等。

- **编辑距离法**：给定两个域名A和B，该方法计算从A转换到B所需的最小编辑次数，编辑距离越小，则相似度越高。
- **Jaccard相似度法**：两个域名字符集的交集大小除以并集大小。比值越大，则相似度越高。
- **最长公共子序列法**：计算两个域名的最长公共子序列的长度。长度越长，则相似度越高。

  注 – 最长公共子序列指的是两个给定序列共有的最长子序列，前提是该子序列的元素无需占据原始序列内的连续位置。公共子序列必须是两个给定序列之索引的严格升序序列。例如，如果“abcde”和“akcve”是两个给定的序列，那么“ace”就是这两个序列的最长子序列。
- **视觉相似度转换法**：在比较之前，替换视觉相似的字符。例如，“0”和“o”可以相互替换；“1”和“i”可以相互替换等，例如，域名“z00.com”就可以转换为“zoo.com”。该方法可以提高相似度的性能。不过，在某些情况下，视觉相似度转换也会降低性能，因此，在转换之前和之后进行相似度比较需谨慎。

7.1.2 官方徽标检测

建议将未知网站中的图像或其他视觉元素与官方徽标进行比较。官方徽标包括但不限于公司或组织的品牌、广告设计和其他标志性元素。官方徽标的检测方法包括以下步骤：

- 检测之前，应该收集官方徽标并将之存储在徽标数据库中。
- 下载或截屏未知网页的视觉元素，并将之与徽标数据库中的徽标进行比较。两个图像之间的相似度可以通过两个流行的描述符来计算，它们是尺度不变特征变换（SIFT）和加速鲁棒特征（SURF）。
- 如果检测网页的源代码已被混淆，那么下载视觉元素可能会很困难。然后可以使用某种基于浏览器的万维网应用程序自动测试框架来截屏网页。在徽标比较之前，可以使用基于人工智能的徽标检测模型来从截屏中裁剪徽标。可以使用一些开源的徽标数据库来把这种基于人工智能的徽标检测模型训练好。

7.1.3 代码混淆检测

欺诈网站可能会混淆恶意或欺诈代码，使之难以被分析。混淆后的代码与普通代码有很大不同。检测混淆代码的方法有很多，包括基于卷积和循环神经网络的分类器等。

- 基于卷积神经网络的分类器可自动提取正常源代码和混淆源代码的n-gram特征。n-gram是来自给定源代码的n个单词的连续序列。单词的数量可设为5或更多，以完全捕获用于分类的判别特征。
- 基于循环神经网络的分类器主要基于长短期记忆（LSTM）网络或变换网络。这些分类器将源代码视为一个字符序列，自动识别正常代码与混淆代码之间的序列模式，而后确定它是否是一个混淆代码。

7.1.4 证书输入检测

证书输入通常以“输入表单”的形式存在于网页的源代码中。输入表单的源代码中通常会有一个“密码”属性（该属性保证用户输入时不显示密码的内容）。可以使用正则表达式或网页分析工具来快速定位这些属性信息。如果网站源代码被混淆，那么可以使用光学字符识别（OCR）方法来检测网站截屏中的证书输入。OCR方法将首先定位网页截屏中的文本区域，然后将文本区域转换为文本。如果转换后的文本包含一些关键字，例如“密码”，那么在网页中检测到证书输入。

7.1.5 第三方安全服务

建议运营商使用第三方安全供应商提供的安全服务来获取网站的属性和统计数据，包括网站流量、声誉、插件、域名注册、认证和其他安全信息。该信息可用作用于确定欺诈网站的附加信息。

7.1.6 链接分析

欺诈网站可能会复制官网中的超链接，来在其欺诈网页中重用官网的视觉元素。该行为可通过链接分析来检测。链接分析收集官网上视觉元素的链接，并与要检测的网站上的链接进行比较。如果两个网站有相同或很多相同的超链接，那么就有可能是一个潜在的欺诈网站。

7.1.7 基于信誉评分的最终识别

建议运营商使用人工智能（AI）决策模型来综合以上建议之对策的所有分析或检测结果，并就一个网站是否为一个欺诈网站做出综合判断。在人工智能决策模型中，每个对抗措施的权重都是在训练阶段后自动确定的。

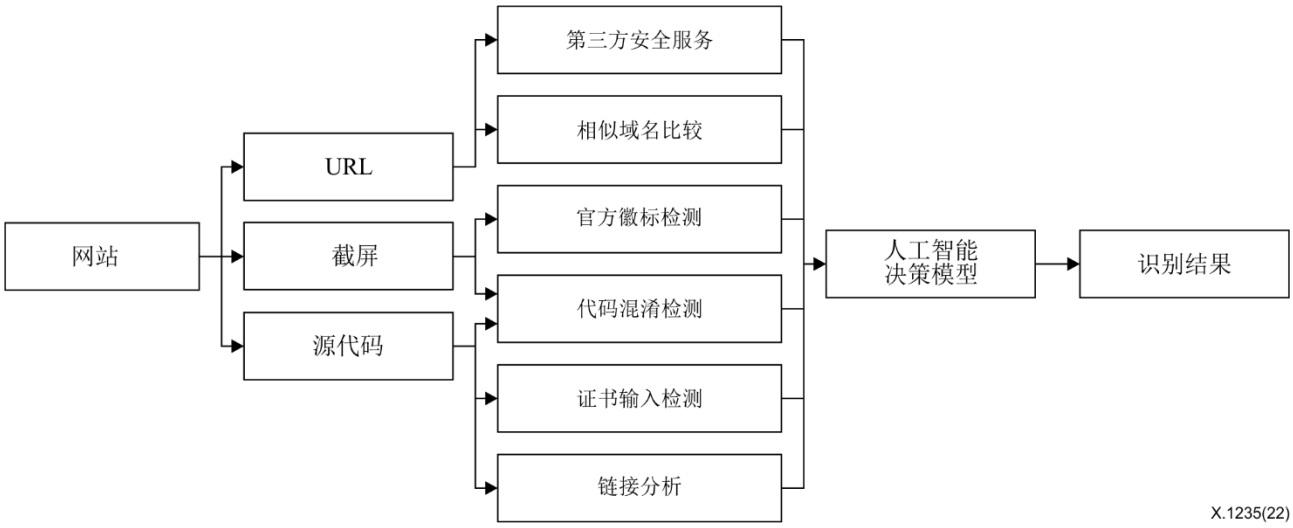


图7-1 – 基于信誉评分的最终识别

如图7-1所示，根据其URL、截图和源代码对网站进行分析。对网页URL，计算域名相似度得分并检查第三方安全服务的结果。对屏幕截图，检测和分析官方徽标和证书输入。对源代码，检测证书输入并执行链接分析。为了确定网站是否被欺诈，人工智能决策模型应该考虑所有这些方面。

为了训练该人工智能决策模型，应该收集所有需要保护的官方网站、已知的欺诈网站和其他正常网站作为样本。所有样本（即收集到的网站）都按照上面建议的对策进行评分，如图7-1所示，每个样本都会有一个评分向量。所有这些评分向量和所有样本类型（欺诈的或

非欺诈的）都可以作为训练数据来训练分类器，以形成人工智能决策模型。分类器可以是基于支持向量机（SVM）或基于深度神经网络的分类器。

通过人工智能决策模型确定的欺诈网站由人工审核员进行审核以避免错误识别，这将是有意义的。

7.2 保护

建议运营商在征得用户同意的情况下采取下列对策来保护用户：

- 警告用户：一旦用户访问已知的欺诈网站，建议运营商暂缓请求，重定向到警告页面，以警示欺诈风险，并要求用户确认请求。
- 创建拦截清单：建议运营商创建一个有关欺诈网站的拦截清单，以中断拦截清单上的所有请求。拦截清单可以在运营商网络的网关或运营商的DNS服务器或其他适当的网络实体中提供服务。
- 防止传播：建议运营商阻断含有至欺诈网站链接的堵塞消息。
- 指导用户防范可疑的欺诈网站：定期提醒用户欺诈网站的风险和特征，提示用户避免使用欺诈网站的最佳做法。建议的最佳做法包括：
  - 不要点击电子邮件或消息中的奇怪链接。
  - 仔细观察地址栏中的域名信息，并与官网进行比较。
  - 使用网页浏览器的安全功能来检查网站的真实性。
- 通过发现同一个欺诈网站的活动域名来保护用户：可使用一个欺诈网站的一组域名来预测该网站的其他活动域名。如果新的活动域名下的网站内容与已知欺诈网站的内容相符，那么可直接将之视为同一个欺诈网站，并采取上述建议的保护措施。

8 机制

建议结合第7节中的所有对策来建立一种系统的、用于对抗欺诈网站的机制。

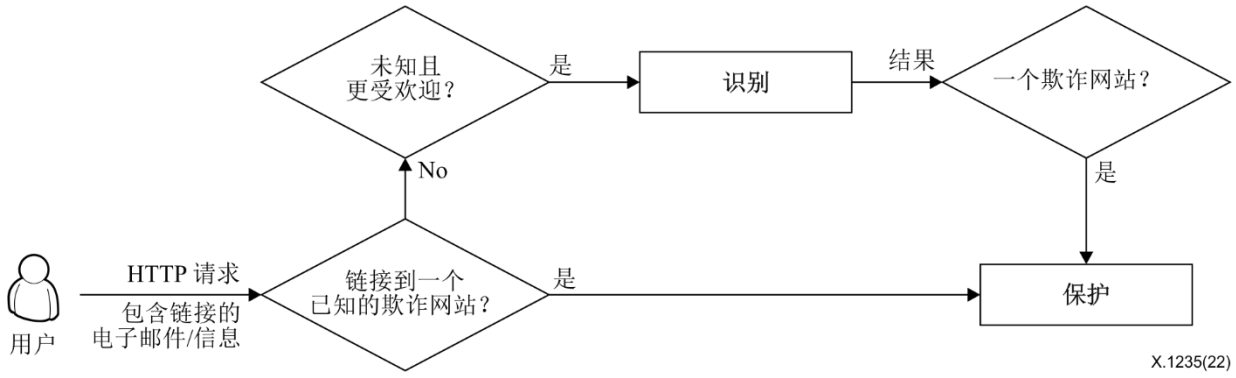


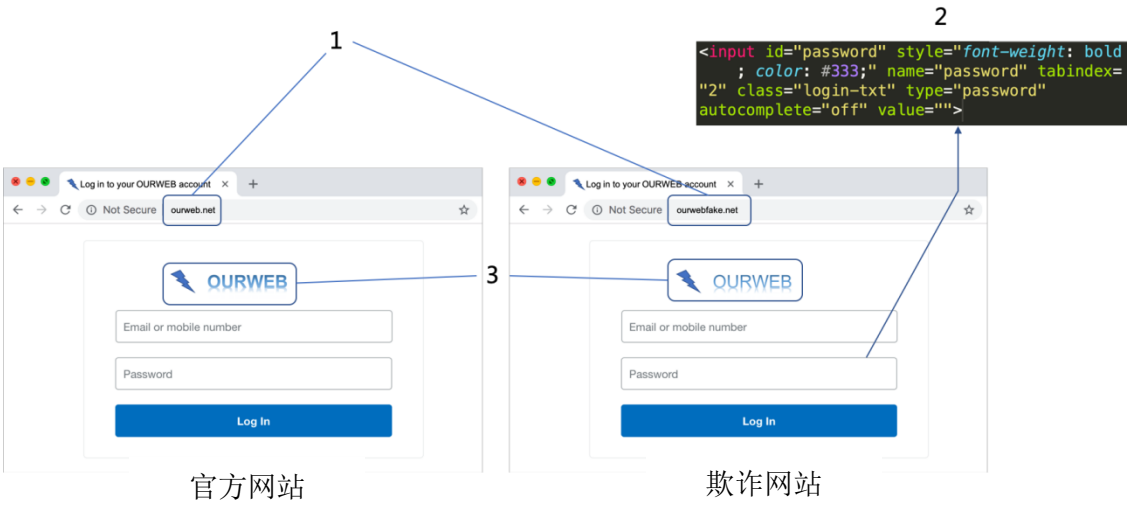
图8-1 – 一种对抗欺诈网站的机制

1) 如图8-1所示，URL可能来自用户的HTTP请求或用户的电子邮件或即时消息（由第三方共享或由用户授权）。
2) 如果URL指向一个已知网站，那么应采取保护措施来处置请求或消息。
3) 如果URL指向一个流行的未知网站，那么应采取识别措施来识别该网站的类型。
4) 如果识别对策的结果表明是一个欺诈网站，那么应采取保护措施以防用户访问该网站。

附录一

对抗欺诈网站的机制示例

（本附录不构成此建议书的组成部分）



图I.1 – 网站和欺诈网站示例

假设有一个名为OURWEB的知名网站，其域名为“ourweb.net”。黑客试图创建一个域名为“ourwebfake.net”的欺诈网站。假设欺诈网站的域名对运营商而言是未知的，那么当大量用户请求欺诈网站时，该网站就变成了一个流行的未知网站。然后利用识别对策对网站进行处置。如图I.1所示，有三种对策可以用来确定欺诈网站。

1) 两个网站的域名相似。假设相似度得分为0.8，对应于常见字符的比例。

2) 欺诈网站中存在证书输入，它可从源代码中来确定。证书输入得分为1。

3) 欺诈网站徽标与官网相似。假设相似度得分为0.9，即SIFT描述性标识符等常见视觉描述性标识符的比例。

4) 假设其他对策的得分为0。

然后我们可以组成一个得分向量[0.8,0.9,0,1,0,0]。向量中的第一个值是域名的相似度得分，第二个值是徽标的相似度得分，第四个值是证书输入得分。可以将此向量输入到SVM分类器，以获得结果。如果结果表明是欺诈网站，那么将通过保护对策来处置之，以防用户访问该网站。例如，应在运营商网络的网关中将网站的域名添加到阻止清单中。

附录二

技术措施示例

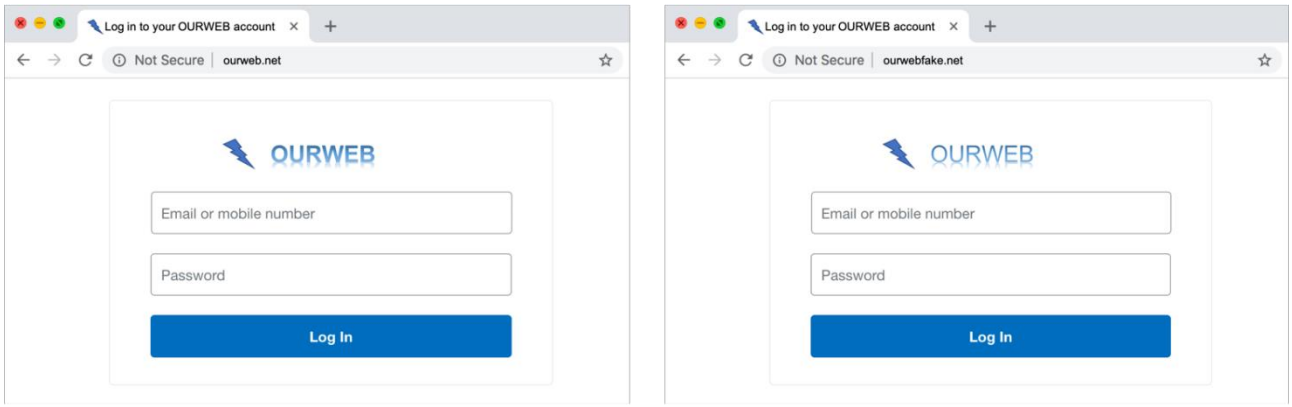
（本附录不构成此建议书的组成部分）

示例II.1：相似域名比较

假设官方域名是“abc123.cn”。欺诈网站使用“abc123cn.org”作为其域名。通过计算两个域名的Jaccard相似度（两个域名字符集的交集大小除以并集大小），我们得到相似度分数8/11 = 0.73。

示例II.2：官方徽标检测

如图II.1所示，左边是OURWEB的官网，右边是对应的欺诈网站。假设将OURWEB的官方徽标添加到徽标数据库中。右边的欺诈网站的徽标与OURWEB的官方徽标非常相似。使用相似度比较算法，可以确定相似度分数（例如，0.9）。



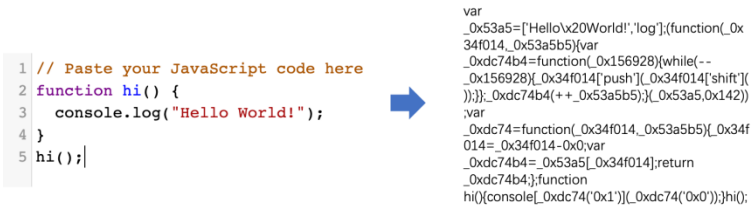
官方网站　　欺诈网站

图II.1 – 带有官方徽标的欺诈网站

示例II.3：代码混淆检测

一些网站使用JavaScript来动态生成网站内容，并使用在线混淆服务（例如，https://obfuscator.io/）来加密JavaScript代码。

如图II.2所示，混淆代码与正常代码明显不同。基于人工智能的文本分类模型可用于预测代码是否被混淆。该算法为源代码提供了一个预测概率值（例如，0.7）。



源代码　　混淆源代码

图II.2 – JavaScript代码混淆示例

示例II.4：证书输入检测

如图II.1所示，欺诈网站诱骗用户输入证书。可以通过检查页面上是否有用于输入证书的表单来对网站进行评分。如果有用于输入证书的表单，那么该站点的得分为1，否则得分为0。

示例II.5：第三方安全服务

来自安全供应商的在线URL查询服务（例如，https://www.urlvoid.com/）可以帮助确定某网站是否为欺诈网站。如果检测到的网站被归类为欺诈网站，那么得分为1，否则为0。

示例II.6：链接分析

在图II.1中，徽标可以参考OURWEB官网的资源。链接分析可以确定图片资源来自ourweb.net（不是ourwebfake.net）。如果网站上有至官方图片资源的链接，那么可记1分，否则记0分。

示例II.7：结果组合

欺诈网站的不同方法的得分被组合成一个向量。表II.1是一个网站评分示例。表的第二列形成一个得分向量。可以将该向量输入分类器来确定该网站是否为欺诈网站。

表II.1 – 网站评分示例

识别方法	得分
相似域名比较	0.8
官方徽标检测	0.9
代码混淆检测	0.7
证书输入检测	1
第三方安全服务	0
链接分析	1

表II.2 – 识别方法与欺诈网站特性之间的映射

识别方法	特性
相似域名比较	相似域名
官方徽标检测	视觉上相似 借用视觉元素
代码混淆检测	混淆源代码
证书输入检测	证书输入
第三方安全服务	
链接分析	链接知名网站

参考书目

[b-ITU-T X.1126] ITU-T X.1126建议书（2017年），缓解移动网络中受感染终端负面影响的导则。

[b-ITU-T X.1244] ITU-T X.1244建议书（2008年），IP多媒体应用反垃圾邮件概述。

[b-SVM] 自然生物技术，2006，24(12) 1565-1567：什么是支持向量机?

ITU-T 系列建议书

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦