Threat Modeling of Banking Malware-Based Attacks

Marco Morana
(OWASP Cincinnati) &
Tony Ucedavelez
(OWASP Atlanta/Versprite Inc)

OWASP

AppSec EU,
June 10th 2011
Trinity College
Dublin Ireland

The OWASP Foundation
http://www.owasp.org

Agenda For Today's Presentation

PART I: Threat Scenario of Hacking and Malware

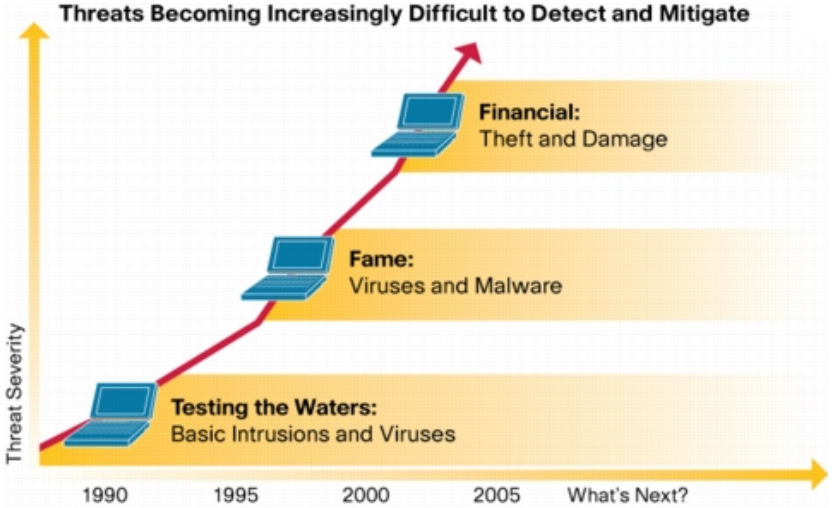
PART II: Presenting The PASTA™ Risk Based Threat Modeling Methodology

PART III: Use of PASTA™ for the analysis of threats, attacks and the managing of risks posed by banking-malware

PART I – Malware and Hacking: The Threat Scenario

The Threat Landscape

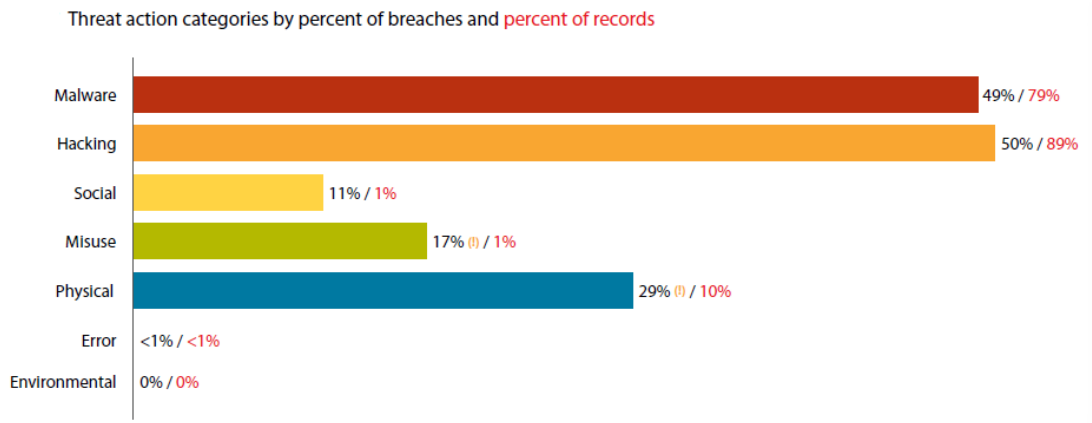
- The threat landscape of cyber attacks has changed dramatically in the last ten years:
  - **Attackers are now financially motivated** examples include theft of credit card data for sale, fraud of bank accounts
  - **Attackers are part of organized crime** that includes gangs of fraudsters, corporate spies, cyber-terrorist groups
  - **Attackers are targeting financial businesses** because is where the money is



SOURCE: Cisco: Threat Control and Containment: New Strategies For A Changed Threat Landscape

Hacking and Malware Threats Stats

- Are the most common threat actions for 2010 data breaches



- Include the top three attack vectors

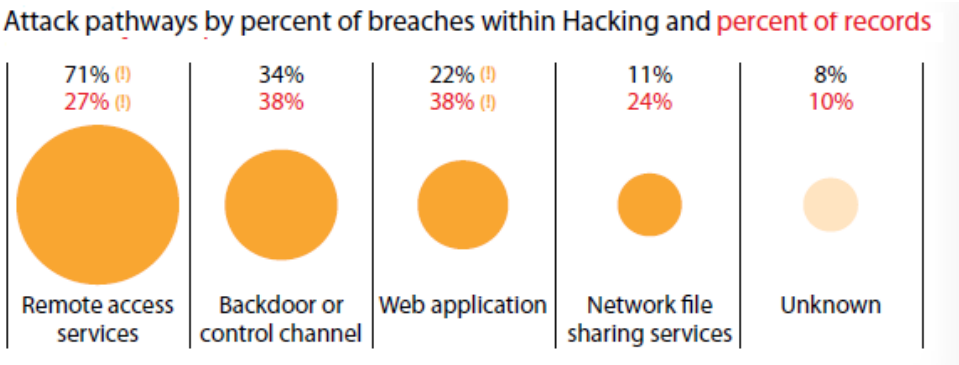
Top 5 Threat Action Types by number of breaches and number of records

	Category	Threat Action Type	Short Name	Breaches	Records
1	Malware	Send data to external site/entity	SNDATA	297	1,729,719
2	Malware	Backdoor (allows remote access / control)	MALBAK	294	2,065,001
3	Hacking	Exploitation of backdoor or command and control channel	HAKBAK	279	1,751,530
4	Hacking	Exploitation of default or guessable credentials	DFCRED	257	1,169,300
5	Malware	Keylogger/Form-grabber/Spyware (capture data from user activity)	KEYLOG	250	1,538,680

Source: Verizon Data Breach investigation Report: http://www.verizonbusiness.com/Products/security/dbir/

Hacking and Malware Attack Paths & Targets

- Web applications are the attack path sought for the highest percentage of data records breached



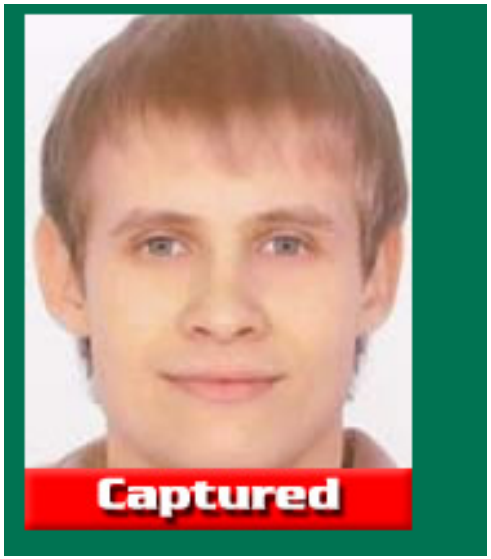
- The top 5 types of data sought by attackers are credit card and authentication data

	Number of incidents	Percent of incidents	Percent of records
Payment card numbers/data	593	78%	96%
Authentication credentials (usernames, pwds, etc)	339	45%	3%
Personal Information (Name, SS#, Addr, etc)	111	15%	1%
Sensitive organizational data (reports, plans, etc)	81	11%	0%
Bank account numbers/data	64	8%	<1%
Intellectual property	41	5%	<1%

Source: Verizon Data Breach investigation Report: http://www.verizonbusiness.com/Products/security/dbir/

The Threat Actors Behind Hacking & Malware

The would-be assailant wakes up, has some coffee (or tea, or maybe even vodka), and begins the workday with a nice compiled list of IPs for vulnerable devices along with the exact usernames and passwords needed to access them. After that, put in a few hours cramming malware onto selected systems, revisit last week's victims to collect some captured data, and then head home early to the wife and kids.



THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS

New York Field Office

Home • New York • Press Releases • 2010 • Manhattan U.S. Attorney Charges 37 Defendants Involved in Global

Manhattan U.S. Attorney Charges 37 Defendants Involved in Global Bank Fraud Schemes that Used "Zeus Trojan" and Other Malware to Steal Millions of Dollars from U.S. Bank Accounts

Defendants Allegedly Compromised Dozens of Accounts and Transferred More Than $3 Million in Stolen Funds to Hundreds of Accounts Opened Under False Identities

U.S. Attorney's Office
September 30, 2010

Southern District of New York
(212) 637-2600

Source: Verizon Data Breach investigation Report: http://www.verizonbusiness.com/Products/security/dbir/
CyberCrime & Doing Time A Blog about Cyber Crime and related Justice issues: http://garwarner.blogspot.com

The New vs. the Old or Dr Jerkill/Mr Hyde vs. Sherlock Holmes

Lesson #1 From Business Risk Management: I Know it By I Ignore it

Lesson #2: Act By Fear, Doubt, Uncertainty

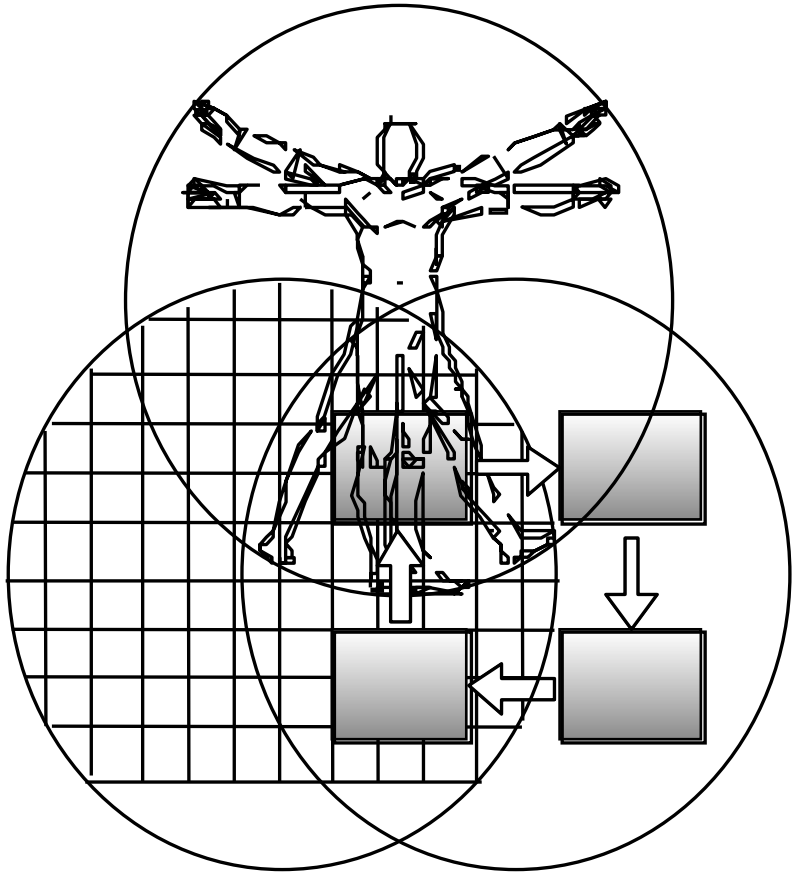
- **Fear of failing audit/non compliance** => additional fines, restrictions and controls (e.g. SEC, PCI etc)
- **Fear of bad reputation/press** => public disclosure of data breach of PII in most US states (SB1386)
- **Fear of lawsuits from businesses** => fraud losses from private's business and customers
- **Doubts on risk mitigation measures** => Not trusting our own security technology, people, processes
- **Uncertainty on business impacts** => Are we the target? How much money we loose from fraud incidents?

Lesson #3: Adopting An Adversarial Approach Toward Risk Management

- "Us vs. Them" (Security vs. Dev/IT/Business) Problem:
  - Remediation is drudgery
  - Demonstrating Threats & Mitigation Techniques is Absent
  - Does not foster collaboration amongst those whose ID risk and those who mitigate it.

Lesson #4 There is a Mature Approach to Risk Management: People, Process, Tools”

- **People** prepared to learn/ deal/respond to cyber threats
- **Processes** for identifying security flaws that exploit weaknesses in applications/controls
- **Tools and countermeasures** to mitigate the risk posed to cyber threats



PART II-Introducing PASTA™ (Process for Attack Simulation and Threat Analysis) Risk Based Threat Modeling Methodology

Threat Modeling Defined

- ***[Application] Threat Modeling***
  - *A **strategic process** aimed at considering possible **attack** scenarios and **vulnerabilities** within a proposed or existing **application environment** for the purpose of clearly identifying **risk** and **impact** levels.*
- Use formal models to categorize threats, map them to vulnerabilities and identify countermeasures
- Different focus for the analysis:
  - Software centric
  - Asset centric
  - Security centric

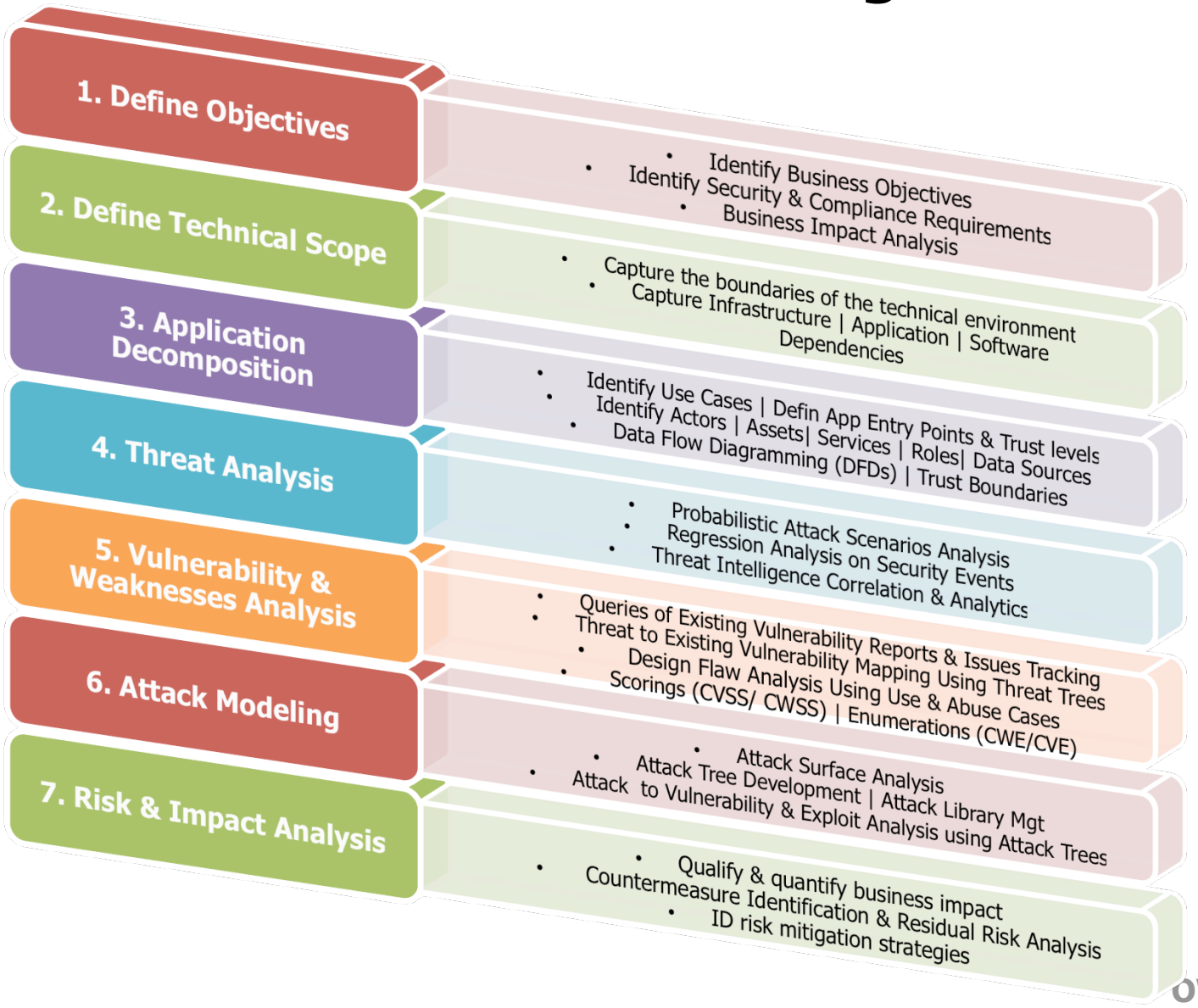
The Limitations of Threat Modeling Today

- **Several methodologies, none is widely accepted**
  - STRIDE & DREAD are not methodologies, threat and risk classification respectively
- **Narrow focus on risk mitigation** (e.g. asset, attack, software, security centric) not all geared toward secure architecture analysis
- **Limited in the adoption within the S-SDLC** comparing with other assessments (e.g. secure code reviews, application pen testing)
- **Not part of IS governance** (e.g. information security risk management, fraud, incident response)
- **Subjective and ad-hoc process** reliant on application security knowledge of SMEs (Subject Matter Experts) /Security Architects/Consultants

The PASTA™ Recipe For Threat Modeling

- Focus on **the application as business-asset target**
- Embodies all **strategic** process for mitigating **cybercrime risks**
- **Simulates attacks and analyzes targets**
- **Implemented in tactical stages** each with pre-determined steps
- **Focused on minimizing risks** to applications and associated impacts to business

The PASTA™ Threat Modeling Methodology



The Beneficiaries of PASTA™ Threat Modeling

- **Business managers** can incorporate which security requirements that impact business
- **Architects** understand security /design flaws and how countermeasure protect data assets
- **Developers** understand how software is vulnerable and exposed
- **Testers** can use abuse cases to security tests of the application
- **Project managers** can manage security defects more efficiently
- **CISOs** can make informed risk management decisions

PART III-Using PASTA™ for threat modeling of banking-malware attacks

Applying P.A.S.T.A for Banking Malware Threat Modeling, Goals of the VII Stages:

I. **Capture requirements** for the risk assessment of banking malware threats, attacks and vulnerabilities

II. **Define the technical scope** for the analysis application and transactions

III. **Conduct architecture level and transactional level security control analysis**

IV. **Identify and extract threat information** from the sources of intelligence/incidents

V. **Analyze weaknesses and vulnerabilities**

VI. **Model attacks scenarios and exploits**

VII. **Formulate a risk mitigation strategy** to reduce the impact of banking malware to the business

STAGE I

Define The Business & Security Objectives:

"Capture requirements for the analysis and management of banking malware risks"

Analysis Of Preliminary Impacts Of Banking Malware

- Impacts to Business
  - **Lose money over fraud** (e.g. illegal money transfers) and loss of customer's sensitive information
  - **Non-liability for fraud against business** accounts triggers lawsuits
  - **Reputation loss** due to either public disclosure of loss of customer's PII (e.g. affect company reputation and customer's loyalty)
  - **Unlawful compliance**, due diligence and failing audit impacts (e.g. PCI-DSS, FFIEC/OCC, GLBA, SB 1386, FACT Act, PATRIOT Act)
- Impacts to the Customers
  - **Theft of credentials**
  - **Theft of sensitive and confidential information**
  - **Loss of money** from business accounts (Business Accounts)

Business Objectives & Security Requirements

Project Business Objective	Security and Compliance Requirement
Perform an application risk assessment to analyze malware banking attacks	Risk assessment need to assess risk from attacker perspective and identify on-line banking transactions targeted by the attacks
Identify application controls and processes in place to mitigate the threat	Conduct architecture risk analysis to identify the application security controls in place and the effectiveness of these controls. Review current scope for vulnerability and risk assessments.
Comply with FACT Act of 2003 and FFIEC guidelines for authentication in the banking environment	Develop a written program that identifies and detects the relevant warning signs – or "red flags" – of identity theft. Perform a risk assessment of online banking high risk transactions such as transfer of money and access of Sensitive Customer Information
Analyze attacks and the targets that include data and high risk transactions	Analyze attack vectors used for acquisition of customers'PII, logging credentials and other sensitive information. Analyze attacks against user account modifications, financial transactions (e.g. wires, bill-pay), new account linkages
Identify a Risk Mitigation Strategy That Includes Detective and Preventive Controls/Processes	Include stakeholders from Intelligence, IS, Fraud/Risk, Legal, Business, Engineering/Architecture. Identify application countermeasures that include preventive, detective (e.g. monitoring) and compensating controls against malware-based banking Trojan attacks

STAGE II

Define The Technical Scope: ”Definition of the scope of the threat modeling exercise”

The Online Banking Application Profile

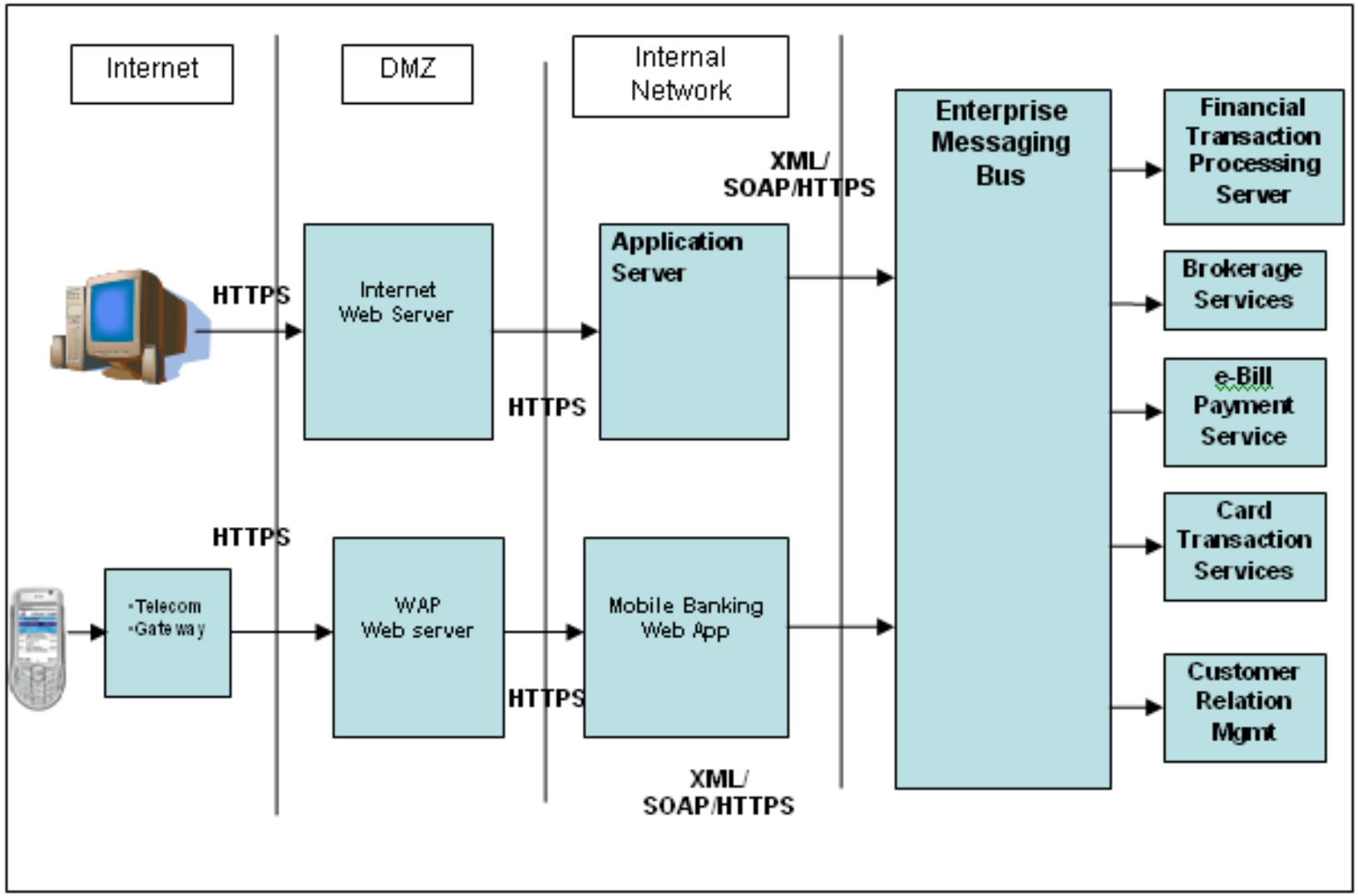
Application Profile: Online Banking Application	
General Description	The online banking application allows customers to perform banking activities such as financial transactions over the internet. The type of transactions supported by the application includes bill payments, wires, funds transfers between customer's own accounts and other bank institutions, account balance-inquires, transaction inquires, bank statements, new bank accounts loan and credit card applications. New online customers can register an online account using existing debit card, PIN and account information. Customers authenticate to the application using username and password and different types of Multi Factor Authentication (MFA) and Risk Based Authentication (RBA)
Application Type	*Internet*
Data Classification	*Public, Non Confidential, Sensitive and Confidential PII*
Inherent Risk	*HIGH*
High Risk Transactions	*YES*
User roles	*Visitor, customer, administrator, customer support representative*
Number of users	*3 million registered customers*

The Definition of The Technical Scope

- Design artifacts used for defining the scope:
  - **Application components** with respect to the application tiers (presentation, application, data)
  - **Network topology**
  - **Protocol/services** being used/exposed from/to the user to /from the back end (e.g. data flow diagrams)
  - **Use case scenarios** (e.g. sequence diagrams)

- Application design information to be extracted to define the scope:
  - **The application assets** (e.g. data/services at each tier)
  - **The security controls of the application** (e.g. authentication, authorization, encryption, session management, input validation, auditing and logging)
  - **The data interactions** between the user of the application and between servers for the main use case scenarios (e.g. login, registration, query etc)

The Architecture Diagram In Scope



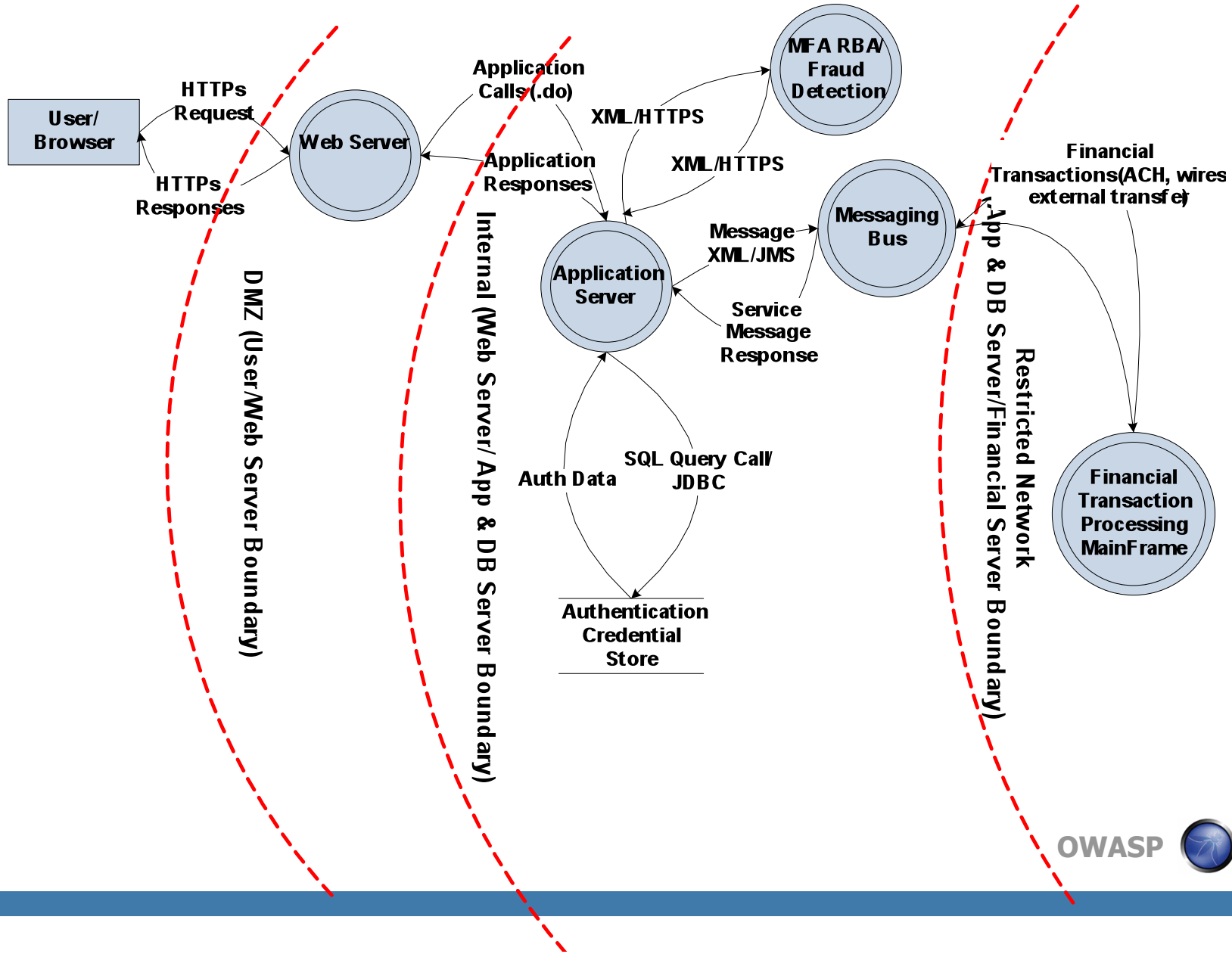
The Application Functions in Scope

- All financial transactions that are possible targets for banking malware attacks:
  - **Login help functions** (e.g. registrations, reset userId/pwd)
  - **Customer profile management functions (**e.g. Change of account profiles, emails, address, phone numbers)
  - **High risk logins** (e.g. authentication with multi-factor authentication)
  - **Transactions involving validation of Sensitive Customer Information** (e.g. Validations of CCN#, CVV, ACC# and PINs for registration/ account opening)
  - **Access of PII and Sensitive Customer Information** (e.g. ACC#, CCN#, SSN, DOB)
  - **High Risk Financial Transactions** (e.g.
    - Money transfers to external accounts
    - ACH
    - Wires,
    - Bill-payments)

STAGE III

Decompose the Application :”Identify the security controls that protect the application data/assets /servers/components”

Data Flow Diagramming



Transactional Security Control Analysis

Online Banking Application Transaction Analysis			Data Input Validation (Initiation)	Authentication/ Identification	Authorization	Session Management	Cryptography (data in rest and transit)	Error Handling	Logging/Audting /Monitoring
Transaction	**Risk**	**Data Classification**	**Security Functions Invoked**						
Password Reset	HIGH	Sensitive	Debit Card, PIN,Account#	Challenge/ Questions Risk Interdicted	Pre-Auth/Bank Customer	Pre-auth SessionID/ Cookie	HTTPS	Custom Errors & Messages	Application, Fraud Detection
Username Recovery	HIGH	Sensitive	Debit Card, PIN,Account#	Challenge/ Questions Risk Interdicted	Pre-Auth/Bank Customes	Pre-auth SessionID/ Cookie	HTTPS	Custom Errors & Messages	Application, Fraud Detection
Registration	MEDIUM	Confidential PII & Sensitive	Debit Card, PIN,Account#, PII (e.g. SSN), Demographics	OOB/ Confirmation	Visitor	Pre-auth SessionID/ Cookie	HTTPS	Custom Errors & Messages	Application
Logon	HIGH	Confidential PII & Sensitive	Username /Password	Single Auth + Challenge/ Questions Risk Interdicted	Post-Auth/Bank Customer	Post-auth SessionID Mgmt	HTTPS/ 3DES Token	Custom Errors & Messages	Application, Fraud Detection
Wires	HIGH	Confidential PII & Sensitive	Amount,Accou nt#, IBAN/BIC	Single Auth + C/Q Risk Interdicted + OTP	Post-Auth/Bank Customer	Post-auth SessionID Mgmt	HTTPS	Custom Errors & Messages	Application, Fraud Detection
Bill Pay	HIGH	Confidential PII & Sensitive	Amount, Payee Account#	Single Auth + C/Q Risk Interdicted + OTP	Post-Auth/Bank Customer	Post-auth SessionID Mgmt	HTTPS	Custom Errors & Messages	Application, Fraud Detection

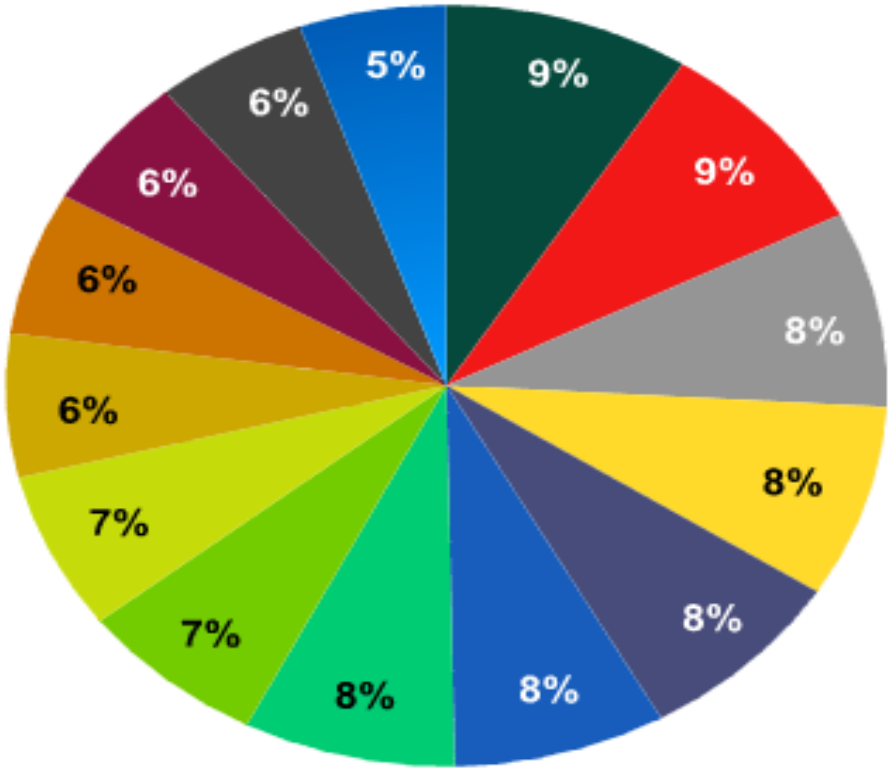
STAGE IV
Identify And Analyze The Threats:
"Identifying and extracting threat information from sources of intelligence to learn about the threat-attack scenarios and attack vectors used by banking malware"

Identification of the Sources Of Intelligence

- **Internal sources** of fraud cases, attacks and incidents (e.g. SIRT)
- **External sources** of gathering and sharing information about banking malware attacks and incidents, these includes public /free and private/at cost services some examples:
  - APWG
  - CERT
  - Digital PhisNet
  - FS-ISAC
  - IC3
  - Internet Fraud Alerts (ifraudalert.org)
  - Trusteer
  - UK Payments Administration
  - Verizon
  - Verisign iDefense
  - Zeus Tracker

Statistical Data Of Banking Malware Targets

Kaspersky Lab

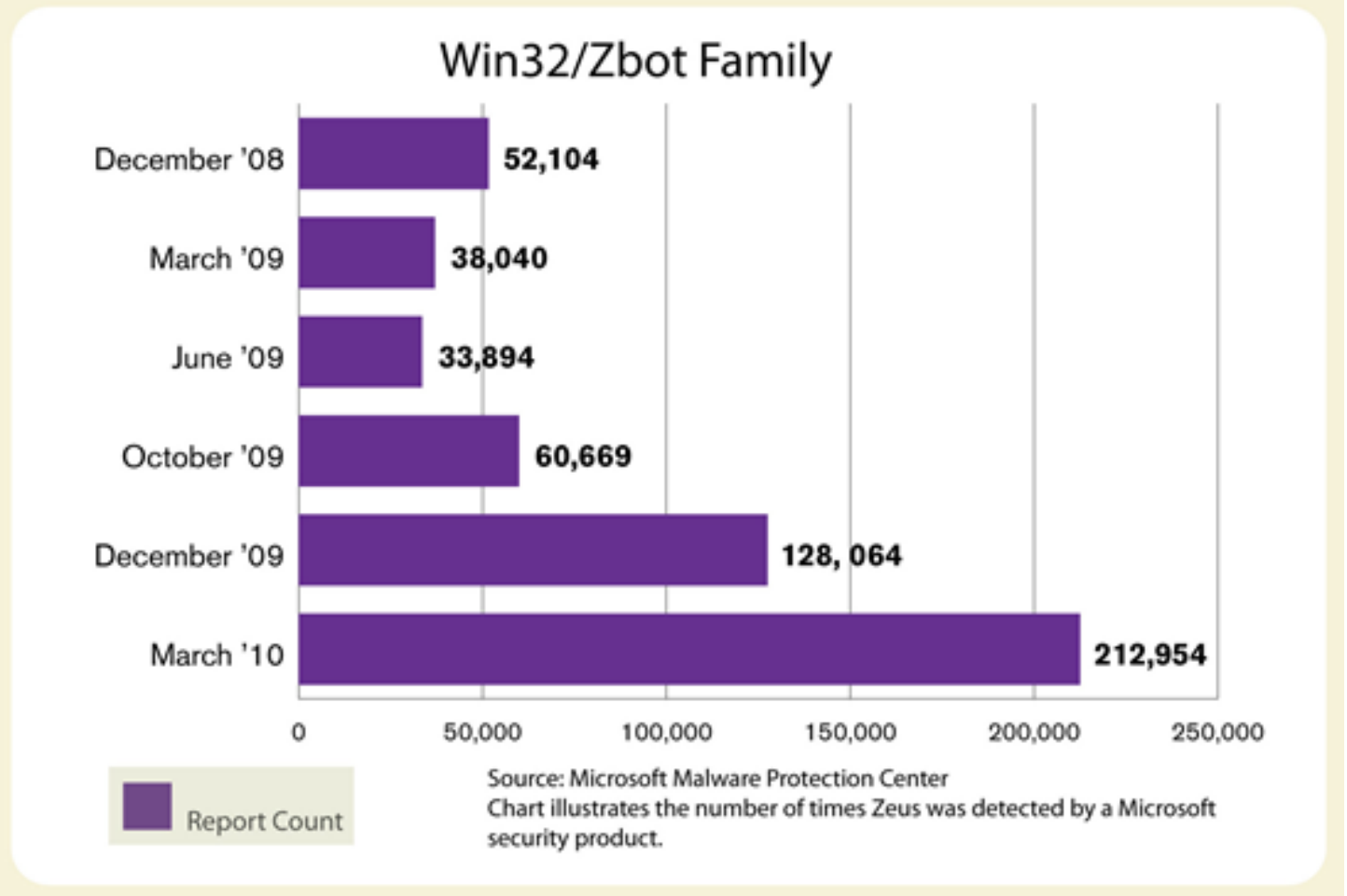


- firstdirect.com
- bankofamerica.com
- citibank.com
- paypal.com
- hsbc.com
- nwolb.com
- rbsdigital.com
- bbvanetoffice.com
- ebay.com
- barclays.com
- uno-e.com
- e-gold.com
- anz.com
- bancajaproximaempresas.com

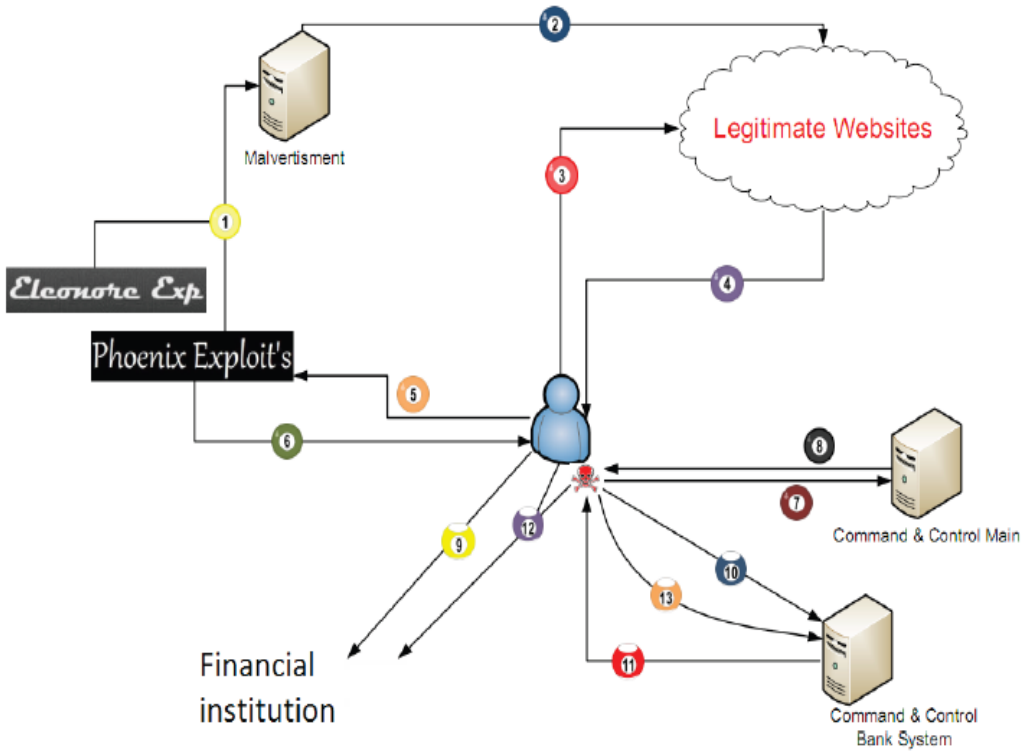
The top-level domains most commonly targeted by ZeuS

OWASP

The Upward Trends Of Spreading of Banking Malware

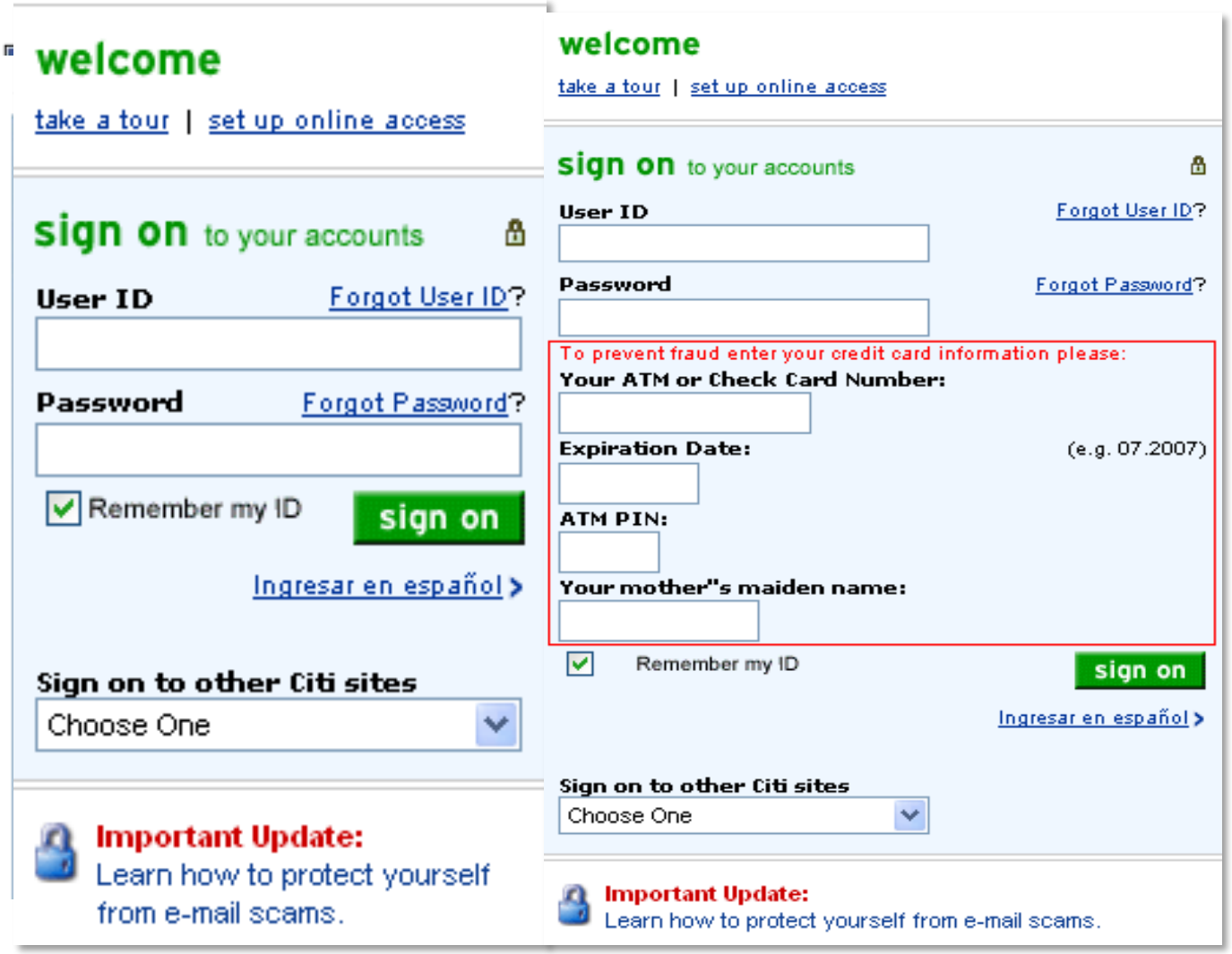


Banking Malware Attack Scenarios



1. Uploads malicious ads to legitimate and fraud ad servers
2. Malicious Ads published on legitimate websites
3. User accesses infected website
4. Website content contains redirection to exploit kit
5. User is redirected to exploit kit
6. User's PC exploited and payload downloaded successfully
7. Trojan reports in to C&C server
8. C&C server sends instructions to trojan
9. User accesses FI web site
10. Trojan reports on user activity to C&C server
11. C&C server sends commands to manipulate transaction
12. Bank transaction is altered to unauthorized payee
13. Trojan reports back success/fail to C&C server

Examples Of Banking Malware Customer Reported Incidents

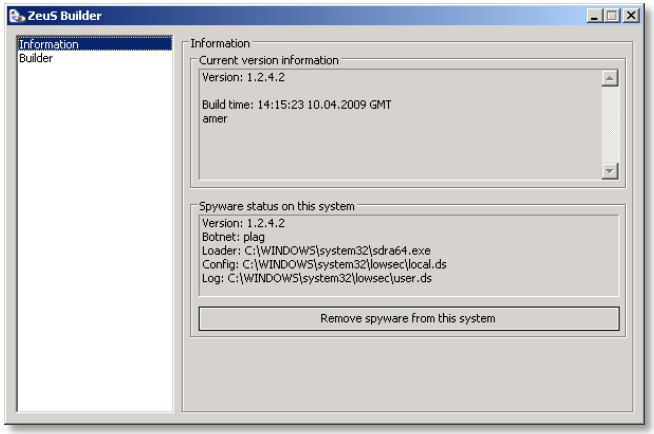


Analysis of Attack Vectors Used By Different Types of Banking Malware

	Infection Method					Attack Capabilities										Timing		Type	
Trojan	Phishing	Drive-by Download	Malicious Web Link	Malicious Ad	Virus Infection	HTTP Injection	Browser Redirect	Form Grabbing	Credential Theft	Keystroke Logging	By Pass MFA	Screen Capture/Video	Certificate Theft	Install Backdoor	Instant Message	Real-Time	Out of Band	Automated	Manual
MB- MitB MM-MitM B-Both O-Other						MB	MM	B	B	B	B	O	O	O	O				
ZeuS	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
SpyEye	*	*	*	*	*	*	*	*	*	*	*	*		*		*	*	*	*
InfoStealer	*	*	*	*	*	*		*	*	*	*	*	*	*			*		*
SilentBanker	*	*	*	*	*	*	*	*		*	*	*	*	*		*	*		*
URLZone	*	*	*	*	*	*		*		*	*	*		*		*	*	*	*
Clampi/Bugat/ Gozi	*	*	*	*	*	*				*							*		*
Haxdoor	*	*	*	*	*	*		*		*				*			*		*
Limbo	*	*	*	*	*	*		*		*	*			*			*		*

Characterizing The Banking Malware Threat Profile

1. **Targeted and customizable**
2. **Uses multiple avenues of infection** a different attack vectors
3. **Takes & sends commands** from command and control server
4. **Evades defenses for client and web application** such as Anti-Virus, SS/TLS, MFA C/Q and fraud detection systems
5. **Injects HTML code into the victim's browser** to harvest accounts, login and PII data while user is logged
6. **Steals certificates** for authentication
7. **Steals user input** with key-loggers and form grabbers
8. **Allows fraudster to transfer money from the victim** machine by riding the user session



STAGE V

Weakness and Vulnerabilities Analysis:

Analyzing application weaknesses and vulnerabilities exploited by banking malware attacks

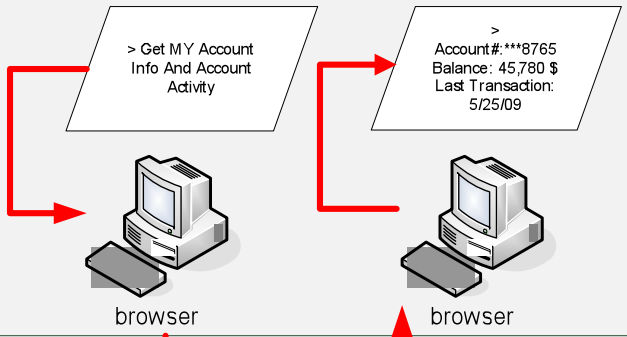
Banking Malware Threats, Vulnerabilities & Application Weaknesses Exploits

- Social Engineering/Phishing Threats
  - Exploit weak anti-phishing site to user controls (e.g. EV SSL)
  - Lack of information to customer on banking malware threats
- Account Takeover & Identify Theft Threats
  - Exploit weak data protection transit & storage (e.g. unsecure cookies, tokens, unsecured secrets and certificates for authentication)
  - Authorization flaws (e.g. RBAC bypass/elevation of privileges)
  - Business logic flaws (e.g. PINs, ACC# validations across channels)
- Financial Loss & Fraud Threats
  - Exploit authentication flaws for transactions (e.g. MFA bypass, weak authentication/factor per transactions),
  - Session management flaws and vulns. (e.g. session fixation, session riding/CSRF)
  - Non repudiation flaws (e.g. one-way SSL no digital signing for transactions)

Architecture Level View Of Security Flaws & Vulnerabilities

Presentation Tier

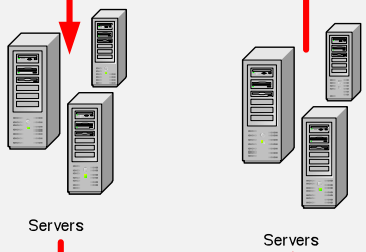
Represents the top most level
of the application .
The purpose of this tier is to translate
commands from the user interface
into data for processing to other tiers and
present back the processed data



Weak Anti-Phishing and Anti-UI-Spoofing Controls & Warnings Browser Vulnerabilities & Flaws

Logic Tier

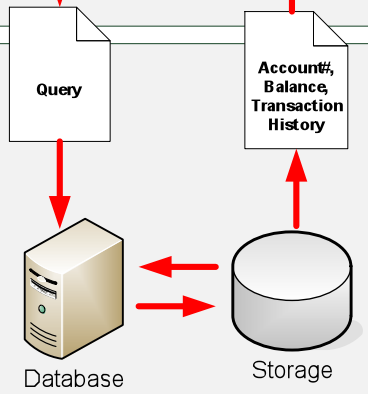
This layer processes commands and
makes decisions based upon
the application business logic
It also moves and processes data
between the presentation and the data tier



Authentication, Authorization, Identification and Session Mgmt. Vulnerabilities and Design Flaws

Data Tier

Is the layer responsible for data storage and
retrieval from a database or file system
Query commands or messages are processed
by the DB server , retrieved from the datasource
and passed back to the lo the logical tier for
processing before being presented to the user



Flaws and Vulnerabilities While Protecting Data/Transaction Confidentiality and Integrity

The Top 5 Malware Propagation Vulnerabilities & The Top 10 Attacks

Rank	BID	Vulnerabilities
1	36299	Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution
2	35759	Adobe Reader and Flash Player Remote Code Execution
3	33627	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution
4	35558	Microsoft Windows 'MPEG2TuneRequest' ActiveX Control Remote Code Execution
5	34169	Adobe Reader Collab 'getIcon()' JavaScript Method Remote Code Execution

Table 2. Top attacked vulnerabilities, 2009
Source: Symantec

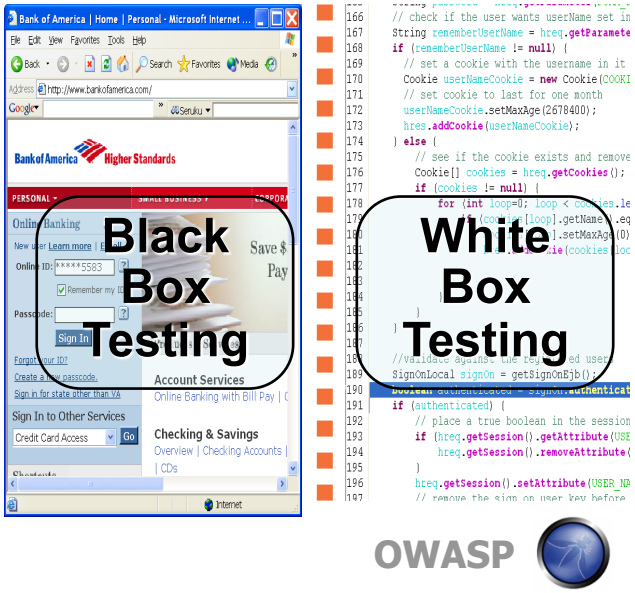
Overall Rank 2009	Overall Rank 2008	Attack	Percentage 2009	Percentage 2008
1	2	PDF Suspicious File Download	49%	11%
2	1	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness	18%	30%
3	N/A	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution	6%	N/A
4	6	Microsoft Internet Explorer MS Snapshot ActiveX File Download	4%	5%
5	4	Adobe SWF Remote Code Executable	3%	7%
6	14	Microsoft Internet Explorer Malformed XML Buffer Overflow	3%	1%
7	5	Microsoft Internet Explorer DHTML CreateControlRange Code Executable	3%	6%
8	20	Microsoft Internet Explorer WPAD Spoofing	3%	1%
9	N/A	Microsoft MPEG2TuneRequestControl ActiveX Buffer Overflow	2%	N/A
10	N/A	Microsoft MPEG2TuneRequestControl ActiveX Instantiation	1%	N/A

Table 3. Top Web-based attacks
Source: Symantec

Web Application Vulnerabilities Likely To Be Exploited By Banking Malware Attacks

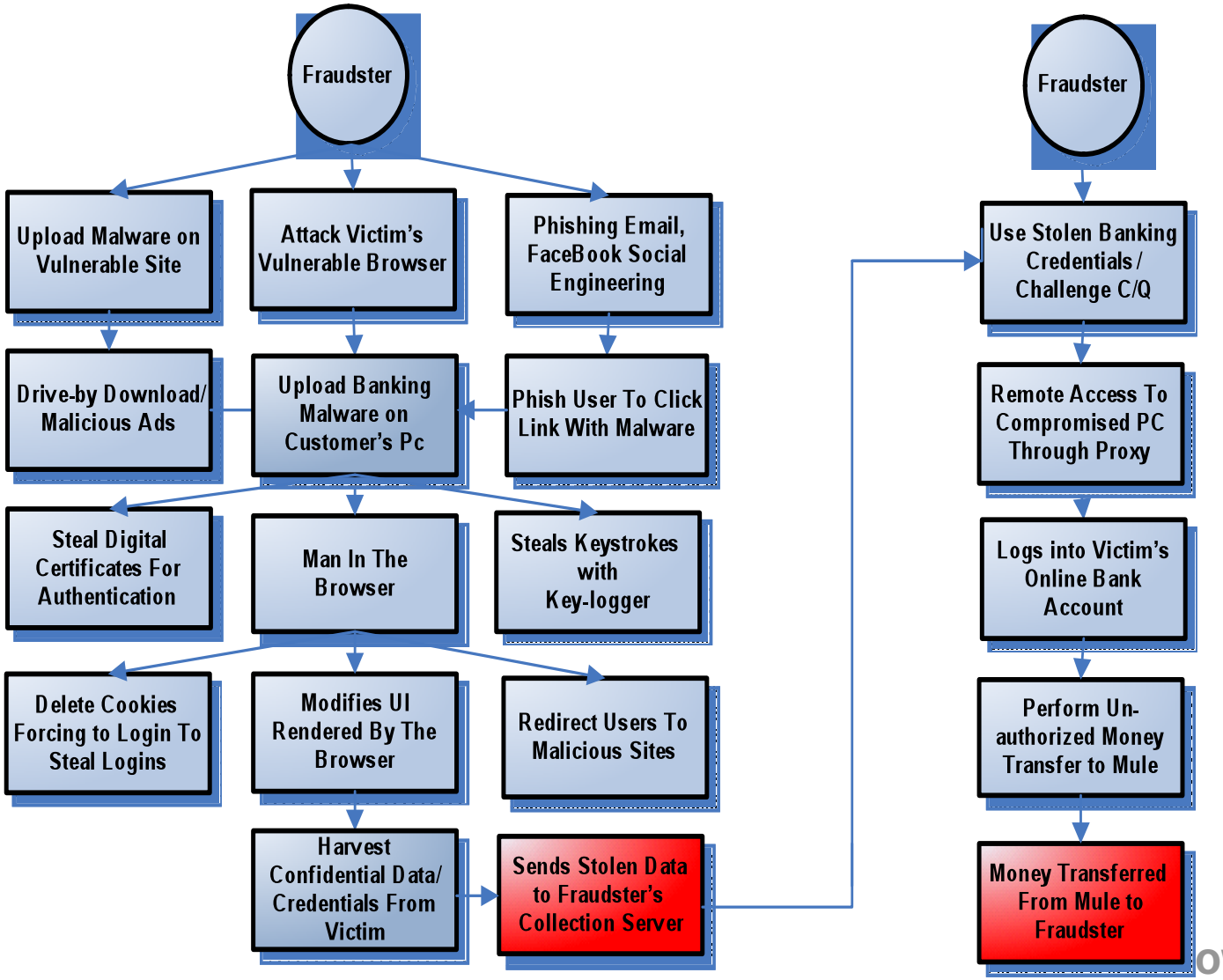
WASC Threat Classification v2	OWASP Top Ten 2010 RC1
WASC-19 SQL Injection	A1 - Injection
WASC-23 XML Injection	
WASC-28 Null Byte Injection	
WASC-29 LDAP Injection	
WASC-30 Mail Command Injection	
WASC-31 OS Commanding	
WASC-39 XPath Injection	
WASC-46 XQuery Injection	
WASC-08 Cross-Site Scripting	A2 –Cross Site Scripting (XSS)
WASC-01 Insufficient Authentication	A3 - Broken Authentication and Session
WASC-18 Credential/Session Prediction	
WASC-37 Session Fixation	
WASC-47 Insufficient Session Expiration	
WASC-01 Insufficient Authentication	A4 - Insecure Direct Object References
WASC-02 Insufficient Authorization	
WASC-33 Path Traversal	
WASC-09 Cross-site Request Forgery	A5 - Cross-Site Request Forgery
WASC-14 Server Misconfiguration	A6 - Security Misconfiguration
WASC-15 Application Misconfiguration	
WASC-02 Insufficient Authorization	A7 - Failure to Restrict URL Access
WASC-10 Denial of Service	
WASC-11 Brute Force	
WASC-21 Insufficient Anti-automation	
WASC-34 Predictable Resource Location	
WASC-38 URL Redirector Abuse	A8 - Unvalidated Redirects and Forwards
WASC-50 Insufficient Data Protection	A9 - Insecure Cryptographic Storage
WASC-04 Insufficient Transport Layer Protection	A10 -Insufficient Transport Layer Protection

OWASP Top Ten 2010 RC1	2010 Top 25
A1 - Injection	CWE-89 (SQL injection), CWE-78 (OS Command injection)
A2 - Cross Site Scripting (XSS)	CWE-79 (Cross-site scripting)
A3 - Broken Authentication and Session Management	CWE-306, CWE-307, CWE-798
A4 - Insecure Direct Object References	CWE-285
A5 - Cross Site Request Forgery (CSRF)	CWE-352
A6 - Security Misconfiguration	No direct mappings; CWE-209 is frequently the result of misconfiguration.
A7 - Failure to Restrict URL Access	CWE-285
A8 - Unvalidated Redirects and Forwards	CWE-601
A9 - Insecure Cryptographic Storage	CWE-327, CWE-311
A10 - Insufficient Transport Layer Protection	CWE-311

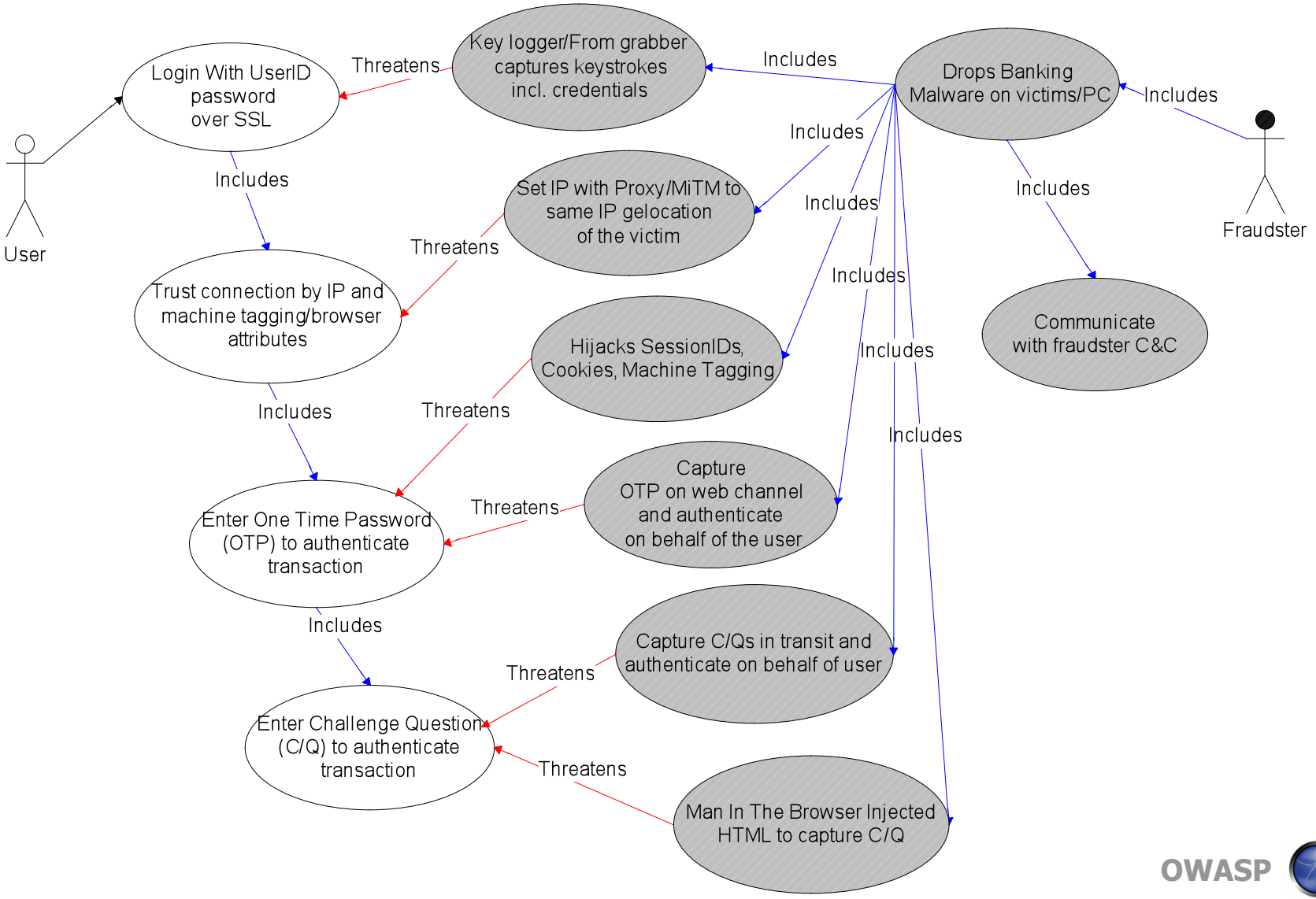


STAGE VI
Model The Attacks and The Exploit Of Weaknesses and Vulnerabilities:
"Modeling of banking malware attacks"

Banking Malware Attack Analysis Using Attack Trees



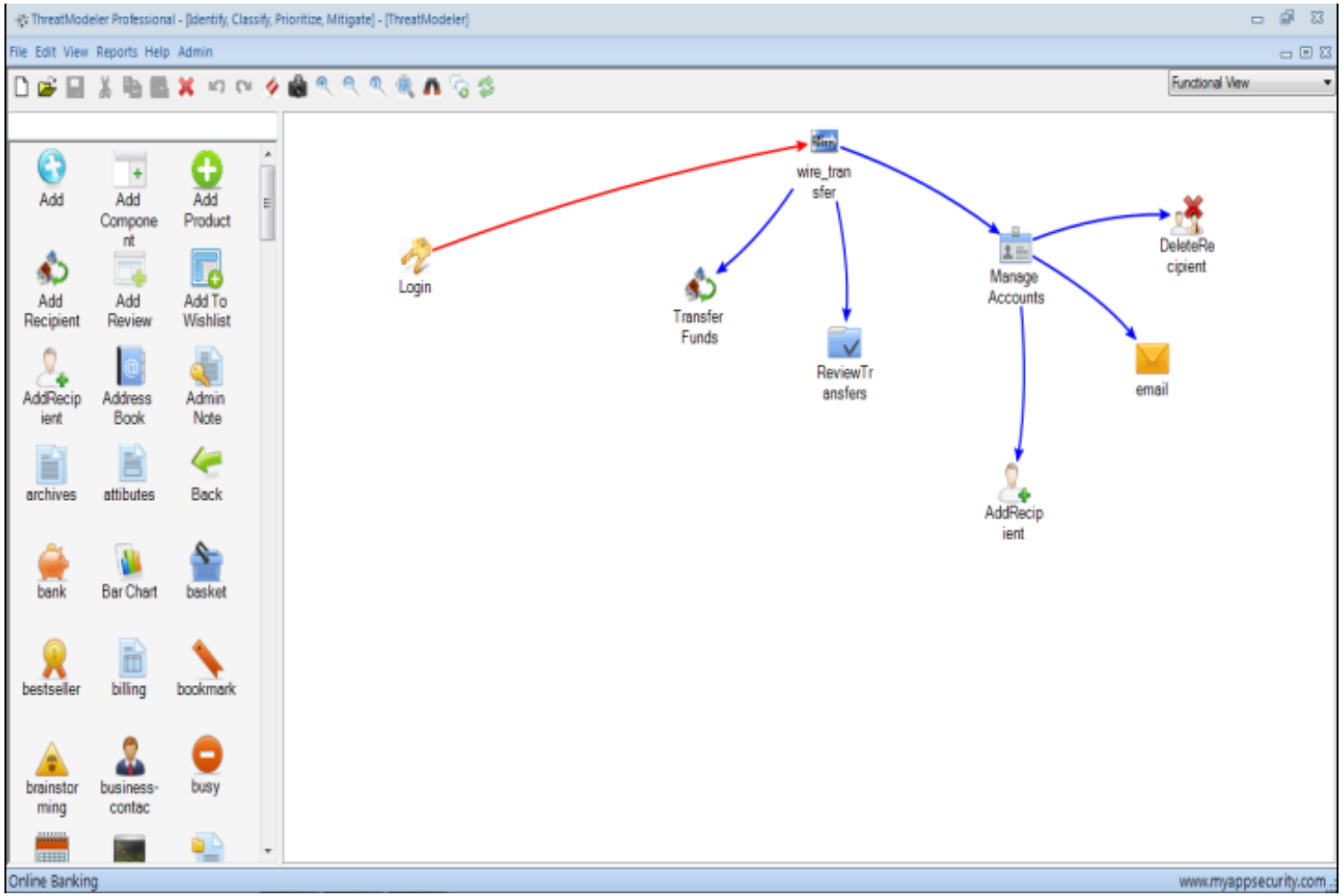
Banking Malware Attack Analysis Using "Use and Abuse Cases"



Attack & Vulnerability Analysis for Application Functions/Transactions

Online Banking Application Security Control Threat Mitigation Gap Analysis			Dropping of Malware via Phishing	Dropping of Malware via Drive By Download	Man in The Browser (MiTB) Attacks	Stealing keystrokes with key-logger	HTML Injection	Certificate/Cookies Theft	Session Hijacking	Man in The Middle (MiTM) Attacks	Un-authorized Money Transfers
Control	**Type**	**Transactions**	**Exploited Vulnerability/Weakness By Attack Vector**								
Single Authentication	Authentication/ Single Factor	Logon	Social Engineering Via Email/ Facebook	Social Engineering Sites/Browser Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Confidentiality of UserID/ Password Browser/Plugin Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Confidentiality/ Integrity of certificate/ cookies used for authentication	Confidentiality of SessionIDs, Session Mgmt Vulnerabilities	Confidentiality/ Integrity of Credentials in Transit Transacton	Bypass single factor authentication to access financial
Security Challenge Questions /Answers	Authentication/ Multi Factor	Password reset UserID recovery Logon Wires Bill pay	Social Engineering Via Email/ Facebook	Social Engineering Sites/Browser Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Confidentiality of challenge Q/A, Browser/Plugin Vulnerabilities	Integrity of Web Forms To Harvest challenge Q/A Browser Security	Confidentiality/ Integrity of cookies for machine Tagging/RBA	Confidentiality of SessionIDs, Session Mgmt Vulnerabilities	Confidentiality/ Integrity of challenge Q/A in Transit Transacton	Confidentiality of challenge Q/A used for financial transactions
One Time Passwords/ Tokens	Authentication/ Multi Factor	Wires Bill pay	Social Engineering Via Email/ Facebook	Social Engineering Sites/Browser Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Confidentiality of OTP Browser/Plugin Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Confidentiality/ Integrity of certificate/ cookies used for authentication	Confidentiality of SessionIDs, Session Mgmt Vulnerabilities	Confidentiality/ Integrity of OTP in Transit Transacton Integrity	Confidentiality of OTP for execution of financial transactions
Account Data Validatons (Debit Card, PIN,Account#)	Data Validation	Registration UserID recovery Passwrod reset	Social Engineering Via Email/ Facebook	Social Engineering Sites/Browser Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Integrity of Account Data Browser/Plugin Vulnerabilities	Integrity of Web Forms To Harvest Account Data Browser Security	Integrity of certificate/ cookies used for pre-auth transactions	Integrity of SessionIDs, Session Mgmt Vulnerabilities	Integrity of Account Data in Transit Transacton Integrity	Integrity of Account data for execution of financial transactions
SessionIDs	Session Management	All transactions	Social Engineering Via Email/ Facebook	Social Engineering Sites/Browser Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Browser/Plugin Vulnerabilities	Integrity of HTTP requests Browser Security Bypass/ Vulnerabilities	Confidentiality/ Integrity of Cookies/ SessionIDs	Confidentiality of SessionIDs, Session Mgmt Vulnerabilities	Confidentiality/ Integrity of SessionID	Impersonation for execution of financial transactions
HTTPS	Encryption Data in Transit	All transactions	Social Engineering Via Email/ Facebook	Social Engineering Sites/Browser Vulnerabilities	Browser Security Bypass/ Vulnerabilities	Confidentiality of key strokes Browser/Plugin Vulnerabilities	Integrity of HTTP requests Browser Security Bypass/ Vulnerabilities	Confidentiality/ Integrity of certificate/ cookies used for authentication	Confidentiality of SessionIDs, Session Mgmt Vulnerabilities	Confidentiality/ Integrity of data in Transit Transacton Integrity	Confidentiality of data for execution of financial transactions

PASTA ™ Threat Analysis With The Help of The ThreatModeler™ Tool

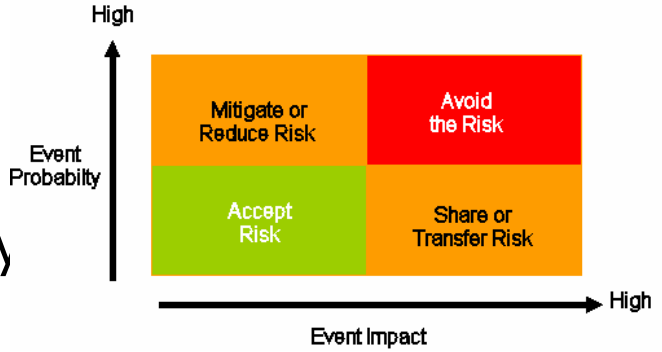


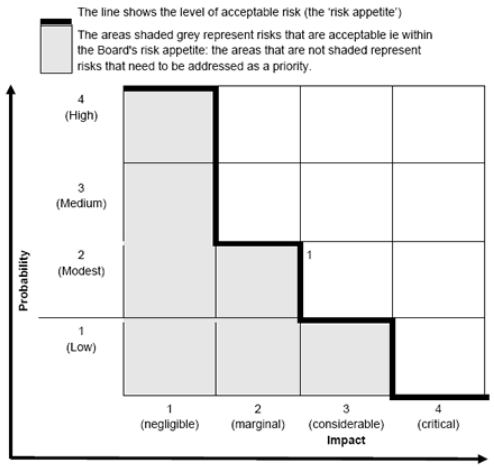
Factors for Managing Risks of Banking Malware Attacks

- **The Threats (e.g. the causes)** Fraudster targeting on-line banking application for data theft and to commit fraud (e.g. un-authorized money transfer to fraudulent accounts)
- **The Vulnerabilities (e.g. the application weakness)** Flaws in authentication and session management; Vulnerabilities in data confidentiality and integrity; Gaps in auditing and logging fraudsters actions and security events
- **The Technical impacts (e.g. compromising security controls)** Bypassing authentication with Challenge/Questions, KBA, OTPs; Bypassing customer validations to authorize financial transactions; Tampering web forms for account takeover Abuse session by impersonating the authenticated user
- **The Business Impact (e.g. financial loss, fraud, fees/fines due to unlawful compliance etc)** Financial loss due to fraud and un-authorized money transfer to money mules; Reputation loss due to disclosure of breaches of customer data, PII; Lawsuits from businesses victim of business account compromise, un-covered money losses; Unlawful non-compliance with regulations

Risk Analysis and Risk Mitigation Strategy

- Calculate risks objectively using different models for calculating risk:
  - **Quantitative** (e.g. Likelihood x Impact (H, M, L), Threat Source (STRIDE) x Severity (DREAD), Threat X Vulnerability Impact (OWASP))
  - **Quantitative** (e.g. ALE = SLE X ARO)
- Devise a risk mitigation strategy based upon holistic measures:
  - **Preventive and detective controls**
  - **Countermeasures at different layers /tiers of mitigation** (e.g. browser web application, infrastructure)
  - **Processes-Governance** (e.g. risk based testing, improved fraud detection, threat analysis, cyber intelligence)





The Banking Malware Risk Management Framework

Threat Agents & Motives	Misuses and Attack Vectors	Vulnerabilities & Weaknesses	Countermeasures	Technical Impacts	Business Impacts
Dropper of Malware seeking to upload it to vulnerable sites	Attacker targets vulnerable sites to upload malware for drive by download	Input validation vulnerabilities allowing for Frame injection of fraudster's URL, file upload via flaws exploits and SQL injection attacks	Identification and remediation of common injection vulnerabilities and data /input validation flaws	Site integrity is violated, visitors of the site get malware downloaded via malicious ads	Reputation loss. Money loss/site taken down, lawsuits
Fraudster attacking bank customers and institutions	Attacker target banking customer with phishing to exploit browser vulnerabilities and upload banking trojan keylogger on his PC/browser	Phishing and social engineering attacks via different channels (email, Facebook, SMS). Lack of customer information about banking malware threats, lack of site to user trust controls (e.g. EV SSL)	Consumer education campaigns, EV-SSL certificates to prove authenticity, site to user controls, browser controls	Once user selects malicious link, JS on client, install banking malware /trojan compromising the browser	Fraud, money losses, reputation loss, data breach disclosure,
Banking malware harvest s viictim's account Data and logins	Banking malware /trojan, inject HTML form fields in session using MiTB attack , keylogger to stead data, sends data to C&C and receives commands	Browser vulns. allowing MiTB, gaps in anti-automation detection controls, virtual keyboard bypassed by form grabbing	Customer education on spoofed Uis, anti-forgey controls, CAPTCHA, Man present controls, anti-forgery controls	Once customer enter extra data in the HTML form it is sent to C&C: loss of data confidentiality and data integrity since outside application control	Loss of customer PII, credentials, PII. Reputational loss via public disclosure of breach, Compliance audit lawsuits, account replacement cost
Fraudster attacking bank customers and institutions	Attacker sends and receives data to banking malware to perform un -authorized financial transactions using MiTM and session riding attacks	Authentication flaws in protecting transaction with adequate strength, session management flaws and vulnerabilities (e.g. session riding/CSFR, fixation), non -repudiation flaws	Architecture risk analysis to identify flaws, OOBA, OOBV, transaction signatures, fraud detection/monitoring, event correlation from logs	Loss of data confidentiality and transaction integrity, session hijacking, missing logging, detection /monitoring and fraud alerts	Money losses associated to fraud from money transfers. Lawsuits compliance/audit risks

Examples of Countermeasures Against Banking Malware Threats

PREVENTIVE

- Anti UI Spoofing/Forging Web Form Controls
  - Watermarks on web forms that are difficult to spoof by the fraudster without the user noticing
  - Customer information to help identify forgery of HTML/injected fields
- Two-Way Out of Band (OOB) Auth & Verification / Transaction Signing
  - SMS, phone to send and receive authorization and verification of transaction

DETECTIVE

- Fraud detection/transaction Monitoring
  - Anomaly detection
  - Detection of cookies HTTP param.
  - Logs of session information x high risk transactions
- Malware vs. Man Present Detection
  - Capture/profile browser actions /events
  - Anti-automation/CAPTCHA
- Customer alerts (e.g. SMS)
  - Real time notification for financial transactions /account changes


QUESTIONS
ANSWERS