



SEC+

Lesson 11:

Enhance Application Security Capabilities

Lesson 11

Topic 11A

Application Protocol
Security Baselines



Secure Protocols

- Many of the protocols used today were developed many decades ago
 - Functionality was primary focus
 - Trustworthiness was assumed
 - Cybersecurity was less of an issue than it is today
- Insecure Protocols
 - Transmit data in clear text format
 - Generally, cannot be secured
 - Must be avoided
- Secure Protocols
 - Same functionality and secure
 - More complex to configure

Insecure	Secure Alternative
Telnet	SSH
HTTP	HTTPS
FTP	FTPS/SFTP

Transport Layer Security

- Most Common Uses
 - Secure HTTP communications
 - Virtual Private Networking (VPN)
- SSL/TLS Versions
 - SSL 2.0, 3.0
 - TLS 1.0, 1.1, 1.2, 1.3
 - Only use TLS version 1.2 or newer
 - Disable all others
 - Downgrade attack

Transport Layer Security

- Cipher Suites
 - Describe the mix of algorithms used to implement TLS protections

- Prior to TLS 1.3

ECDHE-RSA-AES128-GCM-SHA256

- TLS 1.3 uses shortened suites

TLS_AES_256_GCM_SHA384

- Only lists bulk encryption key strength, mode of operation and hash type

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.106	172.217.20.132	TCP	66	53476 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.016952	172.217.20.132	192.168.0.106	TCP	66	443 → 53476 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0
3	0.017028	192.168.0.106	172.217.20.132	TCP	54	53476 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.018272	192.168.0.106	172.217.20.132	TLSv1.3	688	Client Hello
5	0.036762	172.217.20.132	192.168.0.106	TCP	60	443 → 53476 [ACK] Seq=1 Ack=635 Win=62208 Len=0
6	0.036763	172.217.20.132	192.168.0.106	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
7	0.037274	192.168.0.106	172.217.20.132	TLSv1.3	118	Change Cipher Spec, Application Data
8	0.038669	192.168.0.106	172.217.20.132	TLSv1.3	224	Application Data


```
> Frame 6: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) on interface \Device\NPF_{DC478856-D898-4
> Ethernet II, Src: Tp-LinkT_cf:ea:cb (60:e3:27:cf:ea:cb), Dst: Tp-LinkT_15:af:e4 (c4:e9:84:15:af:e4)
> Internet Protocol Version 4, Src: 172.217.20.132, Dst: 192.168.0.106
> Transmission Control Protocol, Src Port: 443, Dst Port: 53476, Seq: 1, Ack: 635, Len: 212
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 128
  v Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 124
    Version: TLS 1.2 (0x0303)
    Random: dba516a7b5f5b3d4f95453c6bbdfe85d73a1db4632640372...
    Session ID Length: 32
    Session ID: 011fa8811607e422d8a3d92ecdd135e6da77498d8b64f75d...
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Compression Method: null (0)
    Extensions Length: 52
  > Extension: pre_shared_key (len=2)
  > Extension: key_share (len=36)
  v Extension: supported_versions (len=2)
    Type: supported_versions (43)
    Length: 2
    Supported Version: TLS 1.3 (0x0304)
```

Viewing the TLS handshake in a Wireshark packet capture. Note that the connection is using TLS 1.3 and one of the shortened cipher suites (TLS_AES_128_GCM_SHA256).

Secure Directory Services

- A Network directory contains
 - Subjects (users, computers, and services)
 - Objects (directories and files) available in the environment
 - Permissions that subjects have over objects
 - High-value attack target

- Lightweight Directory Access Protocol (LDAP)
 - Default is cleartext communication

Simple Network Management Protocol Security

- Simple Network Management Protocol (SNMP)
- Management and monitoring
- SNMP monitor + agents
- Provides very detailed information about systems
- Uses “Community Strings” default “Public” and “Private”
- Can be used to issue commands
- SNMPv3 has secure features, other versions should be avoided

File Transfer Services

- File Transfer Protocol
 - Cleartext
 - Used to host and share files
- SSH
 - Primarily used to access a shell remotely
 - Very versatile protocol
 - Can be used as a tunnel for other protocols
- FTP (SFTP) and FTP Over SSL (FTPS)
 - SFTP is FTP tunneled through SSH
 - FTPS is FTP secured using TLS

Email Services

```
GNU nano 2.2.2 File: /etc/dovecot/dovecot.conf Modified
protocols = imap imaps
#protocols = none

# A space separated list of IP or host addresses where to listen in for
# connections. "*" listens in all IPv4 interfaces. "[::]" listens in all IPv6
# interfaces. Use "*", [::]" for listening both IPv4 and IPv6.
#
# If you want to specify ports for each service, you will need to configure
# these settings inside the protocol imap/pop3/managesieve { ... } section,
# so you can specify different ports for IMAP/POP3/MANAGESIEVE. For example:
protocol imap {
  listen = *:143
  ssl_listen = *:943
}
# protocol pop3 {
#   listen = *:10100
#   ..
# }
# protocol managesieve {
#   listen = *:12000
#   ..
# }
#listen = *

# Disable LOGIN command and all other plaintext authentications unless
[ Read 1280 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^X Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
```

Configuring mailbox access protocols on a server.

- SMTP
 - Cleartext by default
 - Transmit email between systems
 - SMTPS is secure configuration
- Open Relay
 - Improperly configured SMTP server
 - Used to send SPAM
- POP & IMAP
 - Used to access mailboxes
 - Cleartext by default
 - POPS & IMAPS are secure

Email Security

- Sender Policy Framework (SPF)

- Email validation method that helps detect and prevent sender address forgery
- Uses data saved in DNS TXT Records
- Can use to identify “authorized senders”
 - Hosted email
 - Marketing campaigns, etc.

```
L$ dig txt microsoft.com
;; Truncated, retrying in TCP mode.

;<<> DIG 9.18.12-1-Debian <<> txt microsoft.com
;; global options: +cmd
;; Got answer:
;; -->HEADER-- opcode: QUERY, status: NOERROR, id: 55789
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
;; QUESTION SECTION:
;microsoft.com.          IN      TXT

;; ANSWER SECTION:
microsoft.com.  1500   IN      TXT      "fg2t8gov9424p2tduo94goe9j"
microsoft.com.  1500   IN      TXT      "t7s6ee51jrj7wm92k53ihipa"
microsoft.com.  1500   IN      TXT      "google-site-verification=M--Cvfn_YvsV-3Fg6Cp_HfAEj32BmT0cTF4l8XkqpwM"
microsoft.com.  1500   IN      TXT      "google-site-verification=Gf0nTUDATpsk1230J0mX0fsYw-3A0BWWAKSdU0ckgI"
microsoft.com.  1500   IN      TXT      "d365mktkey=SxDf1EZxLVmXv6EZUxzjFFGHOapFSDvTWEIjwQ72twx"
microsoft.com.  1500   IN      TXT      "hubspot-developer-verification=OT05NG1wVNEtODmZ180VNE1LTKyNmQLNDhJMDMxY23JNDAX"
microsoft.com.  1500   IN      TXT      "d365mktkey=QdA792dLCZhaAD0CE2HZGWTzTss0p1sNABhXw1bhmX"
microsoft.com.  1500   IN      TXT      "d365mktkey=63581b7e13hox60tLluagv14"
microsoft.com.  1500   IN      TXT      "google-site-verification=UFG3wr5PWsK8LV029RoXXBBUW0_E6qF1WEWWhetkDY"
microsoft.com.  1500   IN      TXT      "docuSign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"
microsoft.com.  1500   IN      TXT      "d365mktkey=J2QHw9BhdAa3ZKZHB*64daJZxW5Fa0dxDe1xDoYyx"
microsoft.com.  1500   IN      TXT      "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.msft.net include:_spf-a.hotmail.com include:_spf1-neo.microsoft.com -all"
microsoft.com.  1500   IN      TXT      "8BP0XjB2B95EdPhy50/q4CtWp0Uv8zL1t1b1mC4y9YJfLd841ts5QL1E1G5LJ4K01A8p2xmyvFujUvN0g="
microsoft.com.  1500   IN      TXT      "d365mktkey=3uc1cF82cpv750Lk70p0vF2"
microsoft.com.  1500   IN      TXT      "facebook-domain-verification=fwzhbbzwng5fgotc2go5l0c3566"
microsoft.com.  1500   IN      TXT      "google-site-verification=pj0auSprFX0ZS9jnPpa5axowHGCDAl1_86dCqFpk"
```

Displaying the TXT records for microsoft.com using the dig tool. (Screenshot used with permission from Microsoft.)

Email Security

The screenshot shows the DNSChecker website interface. At the top, there's a navigation bar with 'Home', 'All Tools', 'DNS Lookup', and 'Public DNS List'. The main heading is 'DMARC Checker', with a sub-heading 'DMARC check validates your real-time DMARC records and finds problems in them.' Below this is a form where 'microsoft.com' has been entered and validated, showing a 'Success!' message with a green checkmark and the Cloudflare logo. A 'DMARC Lookup' button is visible. Underneath, there are 'Related tools' like 'What is My IP', 'Ping IPv6', 'IPv6 Traceroute Test', and 'Convert IPv6 to IPv4'. A 'More Tools' section contains buttons for various DNS and network checks. The 'DNS Record' section shows a DMARC record: `v=DMARC1; p=reject; pct=100; rua=mailto:itex-rua@microsoft.com; ruf=mailto:itex-ruf@microsoft.com; fo=1`. The 'DMARC Tests' section contains a table with the following data:

Category	Host	Result	
DMARC	microsoft.com	DNS Record found.	🟢
DMARC	microsoft.com	DMARC Record found.	🟢
DMARC	microsoft.com	The record is valid.	🟢
DMARC	microsoft.com	DNS DMARC RUA / RUF domains valid.	🟢
DMARC	microsoft.com	DMARC Quarantine/Reject policy enabled.	🟢

- DomainKeys Identified Mail (DKIM)
 - Sender signs emails using a digital signature
 - Receiver uses a DKIM record in the sender's DNS to verify the signature
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
 - Uses the results of SPF and DKIM checks to define rules for handling messages
 - Provides reporting capabilities
 - Email activity
 - Identify systems sending emails
 - Identify unauthorized activity

Email Security

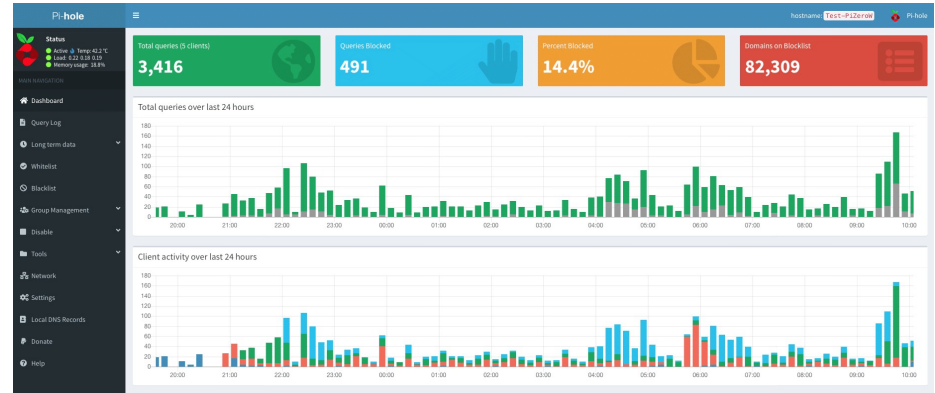
- Email Gateway
 - Control point for all incoming and outgoing email
 - Anti-spam filters and antivirus scanners
 - Sophisticated threat detection algorithms
 - Identify phishing attempts, Business Email Compromise (BEC) Attack
 - Harmful attachments and malicious URLs
 - URL Sanitization/Link Anonymization/Safe Linking/Web Link Transformation
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
 - Encrypts emails to provide the confidentiality and integrity protections
 - Requires Public Key Infrastructure (PKI)

Email Data Loss Prevention

- Email is one of the most frequently used communication channels within organizations
 - Conduit for sensitive data
 - Encourages careless handling of sensitive data (ease of use) and prone to human error
 - Common channel for data loss
 - GDPR, HIPAA, and PCI DSS, (and others) have requirements for protecting data
- DLP scans emails and attachments for certain types of sensitive information
 - Prevents unauthorized sharing of sensitive information
 - Create organization-wide DLP policies
 - Actions are based on predefined rules, such as
 - Blocking the email, alerting the sender, automatically encrypting it

DNS Filtering

- Block or allow access to specific websites
 - DNS filter checks requests against a database of domain names
 - Block access to malicious sites
 - Content/Site Restrictions
 - Ad-blocking (Pi-Hole, AdGuard)
- OpenDNS opendns.com
- Quad9 quad9.net
- CleanBrowsing cleanbrowsing.org
- Cisco Umbrella umbrella.cisco.com/products/dns-layer-network-security
- CloudFlare DNS cloudflare.com/application-services/products/dns/



The Pi-hole administrative dashboard showing DNS resolution statistics. (Screenshot courtesy of Pi-hole.)

DNS Security

- DNS Contains valuable information about hosts on a network
- Internal records should not be accessible from the Internet
- DNS protocol is often exploited to perform data exfiltration
- DNS can be exploited to provide malicious data (ex. Attacker IP instead of real IP)

- DNS Security Extensions (DNSSEC)
 - Mitigate spoofing and poisoning attacks
 - Provides a validation process for DNS responses
 - Authoritative server for the zone creates a "package" of resource records (RRset)

Application Protocol Security Baselines

- Secure Protocols
- Transport Layer Security
- Secure Directory Services
- Simple Network Management Protocol Security
- File Transfer Services
- Email Services
- Email Security
- Email Data Loss Prevention
- DNS Filtering

Lesson 11

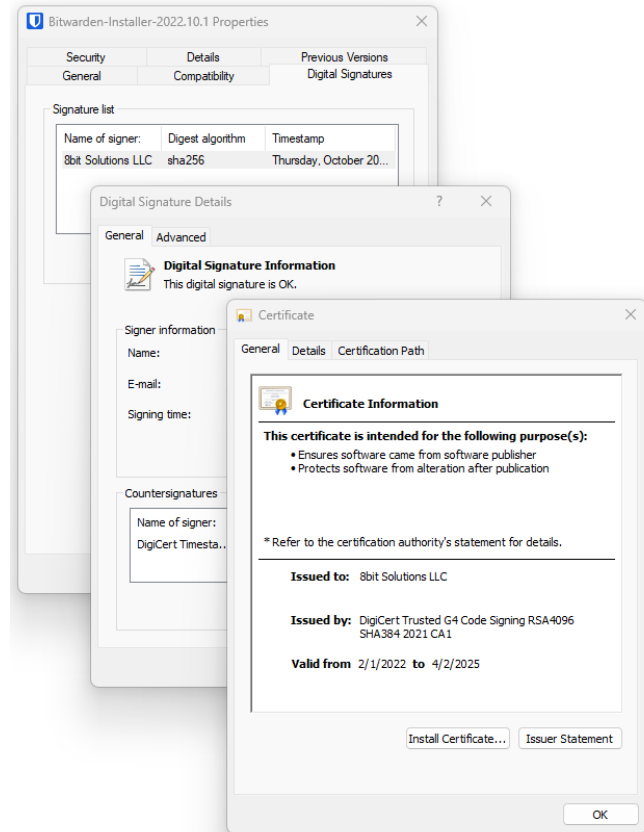
Topic 11B

Cloud and Web
Application Security
Concepts



Secure Coding Techniques

- Pressure to release an application often overshadows the requirement to ensure it is secure
- Coding practices must implement secure development practices
- Code Signing
- Secure Cookies
- Static/Dynamic Code Analysis
- Peer Review



Secure Coding Techniques

- Input Validation
- Attacker provides specially crafted data to an application to manipulate its behavior
- Injection Attack
- Methods used to perform input validation:
 - Allow/Block Lists
 - Data Type checks
 - Range checks
 - Regular Expressions
 - Encoding

Application Protections

- Data exposure
- Allows privileged information to be read by unauthorized user
 - Access token
 - Password
 - Personal data
- Error Handling
 - Safely handle and control errors
 - Report errors to logs instead of user interface
- Application Security in the Cloud
 - Application security supports the shared responsibility model
 - Secure applications running on a secure cloud platform

Application Protections

- Memory Management
 - Buffer overflow attacks are a decades-old problem
 - Input validation is an important defense

- Client-Side vs. Server-Side Validation
 - Security checks should be performed server-side
 - Developers often use client-side checks to improve application performance
 - Client-side checks can be bypassed

Software Sandboxing

JOESandbox Cloud BASIC

Overview Signatures Process Tree Domains / IPs Dropped Static Network Stats Behavior Disassembly

Windows Analysis Report


PO_4260031166.exe

Create Interactive Tour

Overview

General Information

Sample Name: PO_4260031166.exe
Analysis ID: 813695
MD5: 68a113aaecd48a...
SHA1: 865d56042526c...
SHA256: 5fa5c8497d707...
Tags: exe SnakeKeylogger
Info: [Icons]



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

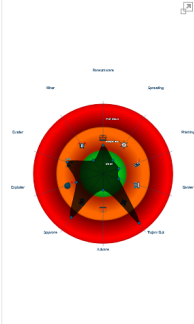
Snake Keylogger

Score: 100
Range: 0 - 100
Whitelisted: false
Confidence: 100%

Signatures

- Multi-AV Scanner detection for submitted.
- Yara detected Snake Keylogger
- Malicious sample detected (through com.)
- Yara detected Telegram RAT
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via file / re...)
- Initial sample is a PE file and has a susp...
- Tries to harvest and steal ftp login creden...
- Machine Learning detection for sample
- May check the online IP address of the ...
- Yara detected Generic Downloader
- Tries to harvest and steal browser inform...
- Uses 32bit PE files
- Queries the volume information (name, s...

Classification



Process Tree

- System is w10x64
- PO_4260031166.exe (PID: 2398 cmdline: C:\Users\user\Desktop\PO_4260031166.exe MD5: 68A113AAECDD8A1C28559CA9BCE29CB2)
- PO_4260031166.exe (PID: 5968 cmdline: C:\Users\user\Desktop\PO_4260031166.exe MD5: 68A113AAECDD8A1C28559CA9BCE29CB2)
- cleanup

Malware Threat Intel

Name	Description	Attribution	Blogpost URLs	Link
404 Keylogger, Snake Keylogger	Snake Keylogger (aka 404 Keylogger) is a subscription-based keylogger that has many capabilities. The info-stealer can steal a victim's sensitive information, log keyboard strokes, take screenshots and extract information from the system clipboard. It was initially released on a Russian hacking forum in August 2019.	No Attribution	<ul style="list-style-type: none">https://blog.netlab.360.com/p...https://blog.miso.eu/2022/04/...https://blogs.blackberry.com/...	https://malpedia.caad.fkie.fraun...

- A security mechanism used to isolate software
- Prevent it from accessing operating system features
- Isolate it from other processes/software
- Prevent access to network
- “Safe Detonation”

- Secure Coding Techniques
- Application Protections
- Software Sandboxing

CompTIA Security+ Exam SY0-701

Lesson 11



Summary

