




Day 2 - Agenda

- HW Solutions
- Basic Constraints flaw
- Void X.509 Flaw
- TLS 1.0 CBC
- BEAST
- Installing SSL in a secure way
- Current Events
- Infamous Attacks
- Additional MITM Tools

Recent Attacks - MSU Direct Deposit Phishing

Date: Thu, 3 Apr 2014 18:32:47 +0000 [04/03/2014 02:32:47 PM EDT]
From: Davis, Thomas <td@MSU.EDU> 
To: CRIMEANDSAFETY@LIST.MSU.EDU 
Reply-To: info@POLICE.MSU.EDU 
Subject: MSU Police Crime Alert

Show this HTML in a new window?

CRIME AND SAFETY ALERT

The Michigan State University Police Department is investigating an attempted theft of employee direct-deposit payroll earnings.

On Tuesday, April 1, it was discovered that a small number of MSU employees had unauthorized changes to their direct deposit information for MSU Payroll. Valid credentials (MSU NetID and password) were used by a perpetrator to modify the employees' banking information on the EBS HR/Payroll (SAP) system. It is believed that the perpetrator gained access to the credentials through a sophisticated "phishing" attack.

There is no indication of a system-wide security breach or exposure of other employee data.

MSU Police are asking anyone who suspects that their banking information has been comprised to call 517-355-2222. Questions related to phishing or MSU NetIDs may be directed to the IT Services Support Desk at (517) 432-6200.

SAFETY TIPS (<http://tech.msu.edu/secureIT>)

Online scammers are becoming much more sophisticated in their attempts to lure victims, especially using email links to false websites. It is increasingly difficult to tell the difference between legitimate and counterfeit online sites. And, unfortunately, there has been a recent increase in phishing attacks at institutions across the country.

Accordingly, each of us must be vigilant in our actions to prevent cybercrime and follow secure practices online:

- Never respond to an email requesting personal information.
- Use a different strong password for each online account.
- Change passwords more frequently for accounts with access to confidential data.
- Never share your password with others.

Learn more by visiting MSU's safe computing website: <http://tech.msu.edu/secureIT>

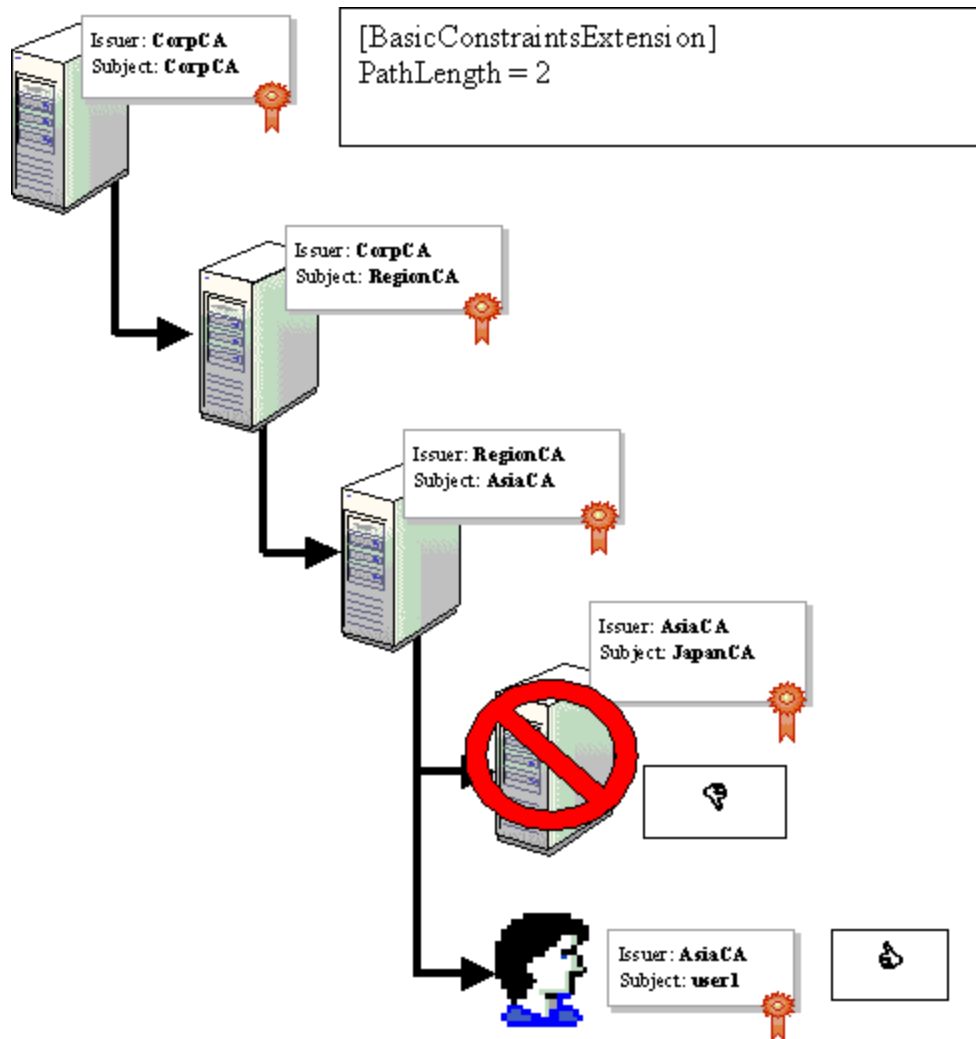
Recent Attacks - Fake ATM Shells

<http://krebsonsecurity.com/2013/12/the-biggest-skimmers-of-all-fake-atms/>



Homework





Certificates - Basic Constraints Flaw

Some web browsers accepted certificates without clearly defined basic constraints

- Allowed end-user certificates to issue other end-user certificates
- IE 6.0
- KDE and Konqueror web browser

Certificates - Void X.509 Flaw

A Null character could be inserted into the Common Name (CN) field

`www.fake.com\0attacker.com` (legitimate)

`www.fake.com`

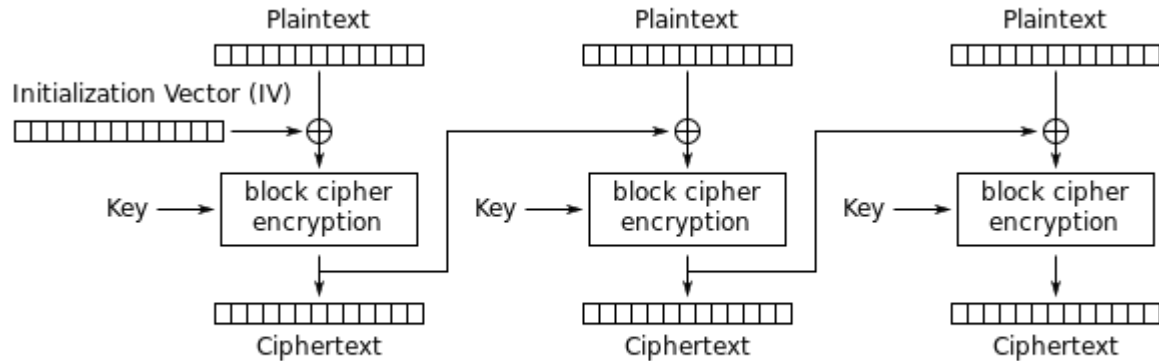
TLS 1.0 Cipher Block Chaining Flaws

Website protocol support

Protocol version	Website support ^[13]	Security ^{[13][14]}
SSL 2.0	23.7% (−0.5%)	Insecure
SSL 3.0	99.4% (±0.0%)	Depends on cipher ^[n 1] and client mitigations ^[n 2]
TLS 1.0	97.7% (−1.6%)	Depends on cipher ^[n 1] and client mitigations ^[n 2]
TLS 1.1	27.6% (+1.9%)	Depends on cipher ^[n 1] and client mitigations ^[n 2]
TLS 1.2	30.2% (+2.0%)	Depends on cipher ^[n 1] and client mitigations ^[n 2]

TLS 1.0 Cipher Block Chaining (CBC)

Initialization Vector (IV)



Cipher Block Chaining (CBC) mode encryption

TLS 1.0 Cipher Block Chaining (CBC)

Initialization Vector (IV) Flaw

Ciphertext = Key(IV XOR Plaintext)

Fix – TLS 1.1 (2006) changed the way the IV was selected

TLS 1.0 Cipher Block Chaining (CBC)

Padding Error Handling

- CBC used blocks of fixed size
 - They pad the last block if necessary

	BLOCK 1 (size : 8 bytes)								BLOCK 2 (size : 8 bytes)							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
PLAIN TEXT	H	E	L	L	O											
PADDED TEXT	H	E	L	L	O	0x3	0x3	0x3								
PLAIN TEXT	H	E	L	L	O	0x20	W	O	R	L	D					
PADDED TEXT	H	E	L	L	O	0x20	W	O	R	L	D	0x5	0x5	0x5	0x5	0x5
PLAIN TEXT	A	S	P	.	N	E	T	!								
PADDED TEXT	A	S	P	.	N	E	T	!	0x8	0x8	0x8	0x8	0x8	0x8	0x8	0x8

TLS 1.0 Cipher Block Chaining (CBC)

Padding Error Handling Flaw Fixes

- The MAC was validated even if the padding failed validation
 - Timing differences persisted
 - Lucky13 attack
- The session was killed if either error returned
 - Possible to circumvent if the attacker could reinitiate the session and the messages appeared in the same position in the stream

SSL / TLS - BEAST Attack

Browser Exploit Against SSL/TLS (BEAST)

- Exploits a well-known CBC vulnerability and web browser SOP flaw to decrypt secret cookies
- Cookie locations are predictable
 - In the HTTP header
 - Usually static

An attacker intercepts a message, decrypts the cookies, then accesses a website posing as the victim

SSL / TLS - BEAST Attack

Countermeasures

- TLS 1.1 and 1.2 fixed the CBC IV flaw
- Disable cross-origin requests on the server-side
- Java 6 and 7 fixed the SOP flaw
- Deny java applet requests to redirect scripts
- Only use HttpOnly cookies
 - Java cannot read or make requests with them
- Restrict of end redirects to third-party content
- Microsoft released a fix in 2012 for Windows 7+

Install SSL in a secure way

Use latest version of OpenSSL

Disable Renegotiation

Only allow High Security Ciphers

Forward Secrecy Ciphers preferred (Available in OpenSSL 1.x)

DHE - Diffie-Hellman

ECDHE - Elliptic Curve Cryptography

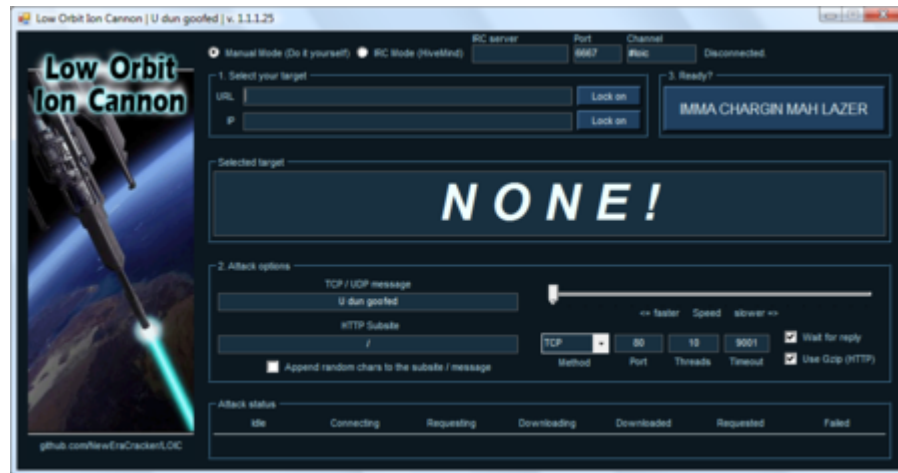
Require the Client to have a Certificate

https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf

Infamous DOS / DDOS Attackers

Anonymous - DDOS

- Originated in 2003 from imageboard. 2008 attacked Church of Scientology
- Coordinated attacks on governments, PayPal, MasterCard, Visa, Sony, Copyright Agencies, etc.
- Commonly used tool for DDOS attack is Low Orbit Ion Cannon



Infamous DOS / DDOS Attackers

lulzsecurity (LulzSec)

- ~11 Members
 - Mainly focused on the Lulz but sometimes had a political message
- Motto: "Laughing at your security since 2011"
- Attacked Corporate and Government servers.
- Released all stolen information to the public
 - This is what lead to their popularity
- 1 Member (Sabu), age 19 from New York was arrested in June 2011
 - His arrest lead to 5 other members being arrested



Infamous DOS / DDOS Attackers

th3j35t3r

- 1 Guy
 - Ex-Military, claims to have served in Afghanistan
 - Focuses attacks on militant jihadi recruiting websites
- He has a Blog: <http://www.jesterscourt.cc/>
- Uses a DOS tool called XerXes, a GUI front end to a DOS script
- He revealed Sabu from Lulzsec real identity
- He has also attacked WikiLeaks, 4chan, and the Ecuadorean stock exchange (He does not like Snowden)
- QR Code Attack via Twitter
 - embedded code inside a QRcode that would connect to a server controlled by the jester.



Additional tools

EtterCap GUI

Webmitm

DNSspoofer + Social Engineering ToolKit

Hamster: Side Jacking

Aircrack-ng

WEP Cracking

WPA Dictionary Attack

